MCIPLab.it

ROMA TRE UNIVERSITÀ DEGLI STUDI

VALUTAZIONE DEL RISCHIO IN SISTEMI INTERDIPENDENTI INDUSTRIALI

STEFANO PANZIERI

ISACA®
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

EMAIL: STEFANO.PANZIERI@UNIROMA3.IT

EVENTO: GESTIONE DEL RISCHIO IN SISTEMI INTERDIPENDENTI: LA PROBLEMATICA CYBER-FISICA

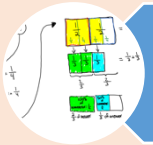
DATA: 29 OTTOBRE 2019

SOMMARIO

Infrastrutture Critiche e Interdipendenze. Effetto Domino

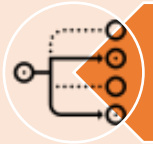
Direttiva NIS

Modellare le Interdipendenze

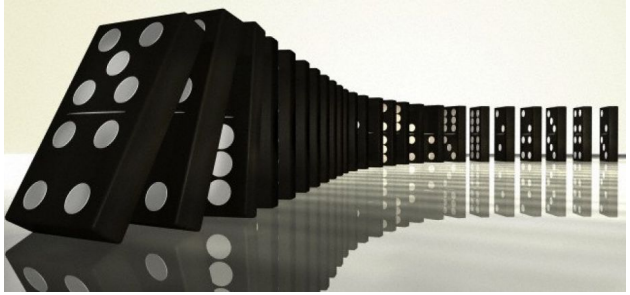


MHR Interdependency model

CISIApro 2.0



A real-time propagation-based approach to risk evaluation



Infrastrutture Critiche e Interdipendenze Effetto Domino

COSA SONO LE INFRASTRUTTURE CRITICHE ?

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Critical Infrastructures are **systems and assets**, whether physical or virtual, so vital for a state that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

[US Patriot Act 2001]

I principali settori critici:

Energia

Salute Pubblica

Trasporti

Acqua Potabile

Telecomunicazioni

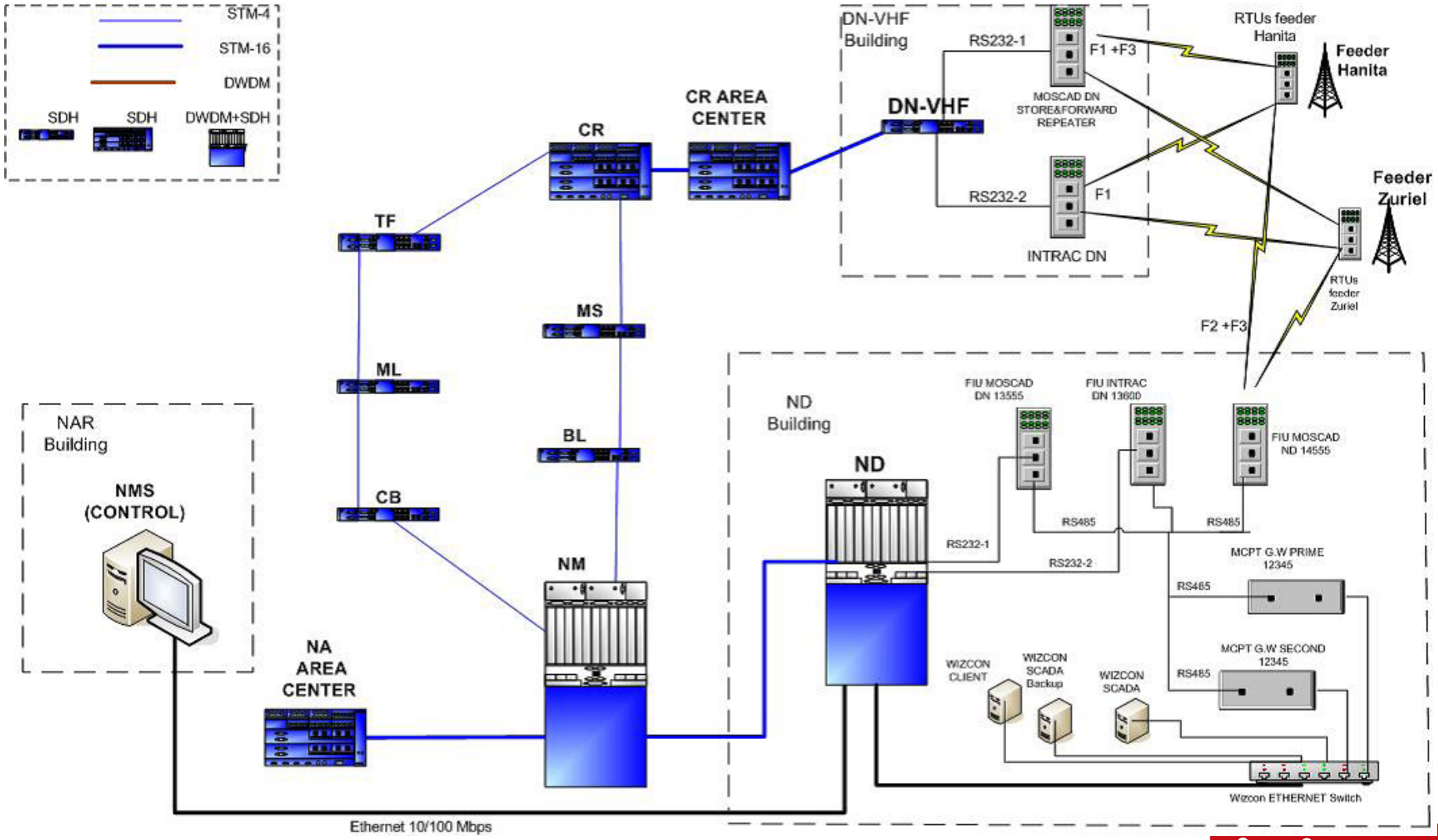
Economia e Finanza

Difesa e Sicurezza

Spazio e Ricerca

MCIPLab.it

CASCADING EFFECTS



Direttiva NIS

DIRETTIVA NIS

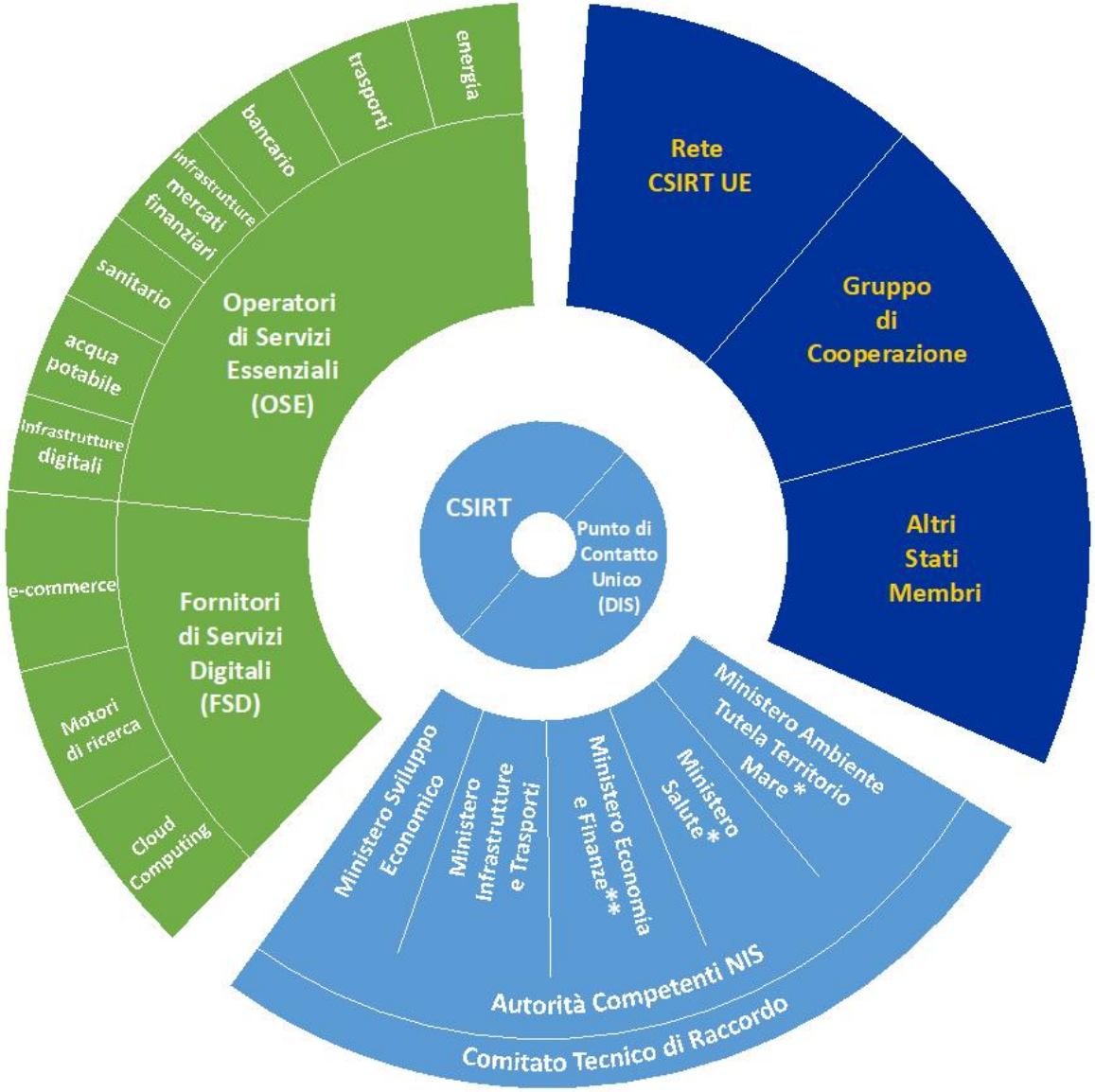
- La direttiva NIS e gli scenari futuri per gli operatori di Infrastrutture Critiche

- **DECRETO LEGISLATIVO 18 maggio 2018, n. 65**
- Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. (18G00092) (GU Serie Generale n.132 del 09-06-2018)
- note: Entrata in vigore del provvedimento: 24/06/2018

STRATEGIA NAZIONALE DI SICUREZZA CIBERNETICA

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

- In ossequio a quanto richiesto dall'Articolo 7 della Direttiva, il decreto di recepimento prevede l'adozione di una strategia nazionale di sicurezza cibernetica da parte del Presidente del Consiglio dei Ministri.
- La strategia dovrà prevedere in particolare le misure di preparazione, risposta e recupero dei servizi a seguito di incidenti informatici, la definizione di un piano di valutazione dei rischi informatici e programmi di formazione e sensibilizzazione in materia di sicurezza informatica.
- **Gran parte di questi elementi sono già affrontati, per grandi linee, nella vigente strategia nazionale di sicurezza cibernetica, delineata nel Quadro strategico nazionale per la sicurezza dello spazio cibernetico del 2013 e ulteriormente sviluppata dal Piano nazionale per la protezione cibernetica e la sicurezza informatica del 2017**.
- **Sarà però necessario aggiornare tale strategia per far sì che tutti gli elementi di cui all'Articolo 7 della Direttiva vengano affronti in maniera specifica e dettagliata, in conformità con i dettami comunitari.**



Servizi interessati

Attori governativi NIS

Meccanismi della cooperazione europea

* più regioni e province autonome di Trento e di Bolzano

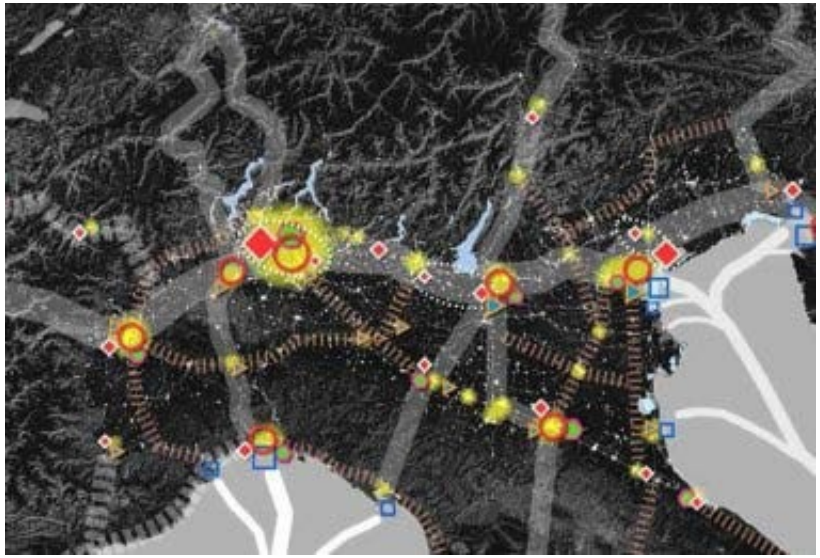
** in collaborazione con le autorità di vigilanza di settore, Banca d'Italia e Consob

CATEGORIA 1/ SERVIZI ESSENZIALI – DEFINIZIONI 1/2

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

❑ Si definisce **«operatore di servizi essenziali»** un soggetto pubblico o privato che soddisfa i seguenti criteri:

- Un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali;
- La fornitura di tale servizio dipende dalla rete e dai sistemi informativi;
- Un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.



❑ **operatori di servizi essenziali** :

- **Settore Energia**
- **Settore Trasporti**
- **Settore bancario**
- **Infrastrutture dei mercati finanziari**
- **Settore sanitario**
- **Fornitura e distribuzione di acqua potabile**

MCIPLab.it

Operatori di servizi essenziali - Obblighi in materia di sicurezza

- Gli obblighi in materia di sicurezza e notifica degli incidenti per gli **operatori di servizi essenziali** prevedono che questi:

1) adottino misure tecniche e organizzative adeguate e proporzionate alla **gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi** che usano nelle loro operazioni;

2) adottino misure adeguate per **prevenire e minimizzare l'impatto di incidenti** a carico della sicurezza della rete e dei sistemi informativi utilizzati per la fornitura di tali servizi essenziali, al fine di assicurarne la continuità;

3) notifichino all'autorità competente o al CSIRT **gli incidenti aventi un impatto rilevante** sulla continuità dei servizi essenziali prestati;

- **L'autorità competente o il CSIRT:**

1) informa l'altro o gli altri stati membri interessati se l'incidente ha un impatto rilevante sulla continuità dei servizi essenziali in quello Stato membro;

2) può informare il pubblico in merito ai singoli incidenti, dopo aver consultato l'operatore notificante dei servizi essenziali;

- Le autorità competenti possono elaborare e adottare orientamenti sulle circostanze in cui gli operatori di servizi essenziali sono tenuti a notificare gli incidenti.

CATEGORIA 2/ SERVIZI DIGITALI - DEFINIZIONI

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

- Si definisce **«servizio digitale»** qualsiasi servizio della società dell'informazione prestato normalmente dietro retribuzione, ovvero qualsiasi servizio a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi, di uno dei seguenti tipi:

- **Mercato online,** servizio digitale che consente ai consumatori e/o ai professionisti, di concludere contratti di vendita o di servizi online con i professionisti sia sul sito web del mercato online sia sul sito web di un professionista che utilizza i servizi informatici forniti dal mercato online;
- **Motore di ricerca online,** servizio digitale che consente all'utente di effettuare ricerche, in linea di principio, su tutti i siti web o su siti web in una lingua particolare sulla base di un'interrogazione su qualsiasi tema sotto forma di parola chiave, frase o di altra immissione, e fornisce i link in cui possono essere trovate le informazioni relative al contenuto richiesto;
- **Servizi nella nuvola (cloud computing),** servizio digitale che consente l'accesso a un insieme scalabile ed elastico di risorse informatiche condivisibili.

- Si definisce **«fornitore di servizio digitale»**, qualsiasi persona giuridica che fornisce un servizio digitale.

FORNITORI DI SERVIZI DIGITALI - OBBLIGHI IN MATERIA DI SICUREZZA

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

- **Gli obblighi** in materia di sicurezza e notifica degli incidenti per i **fornitori di servizi digitali** prevedono che questi:

1) **identifichino e adottino misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano**

Tali misure tengono conto dei seguenti elementi:

a) la sicurezza dei sistemi e degli impianti,

b) il trattamento degli incidenti,

c) la gestione della continuità operativa,

d) la funzione di monitoraggio, audit e test,

e) la conformità con le norme internazionali.

1) **adottino misure per prevenire e minimizzare l'impatto di incidenti a carico della sicurezza della rete e dei sistemi informativi del fornitore di servizi digitali**, al fine di assicurare la continuità di tali servizi;

2) **notifichino senza indebito ritardo all'autorità competente o al CSIRT qualsiasi incidente avente un impatto rilevante sulla fornitura di un servizio** che essi offrono all'interno dell'Unione;

MCIPLab.it

- **L'autorità competente o il CSIRT**:

1) **tutelano**, **la sicurezza e gli interessi commerciali del fornitore del servizio digitale nonché la riservatezza delle informazioni fornite;**
2) **possono informare il pubblico riguardo ai singoli incidenti** o chiedere al fornitore di servizi digitali di provvedervi.

- L'operatore stesso notifica qualsiasi impatto rilevante per la continuità di servizi essenziali dovuto ad un incidente a carico di una eventuale terza parte.

CATEGORIA 3/ SERVIZI DI COMUNICAZIONE ELETTRONICA

La **direttiva *2009/140/CE*** del Parlamento Europeo e del Consiglio del 25 novembre 2009 recante modifica della direttiva *2002/21/CE* che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, «**istituisce un quadro normativo armonizzato per la disciplina dei servizi di comunicazione elettronica**, delle reti di comunicazione elettronica, delle risorse e dei servizi correlati e per taluni aspetti delle apparecchiature terminali onde facilitare l'accesso agli utenti disabili; definisce le funzioni delle autorità nazionali di regolamentazione ed istituisce le procedure atte a garantire l'applicazione armonizzata del quadro normativo nella Comunità».

Rif: Articolo 1, paragrafo 1, della direttiva 2009/140/CE del Parlamento Europeo e del Consiglio del 25 novembre 2009.

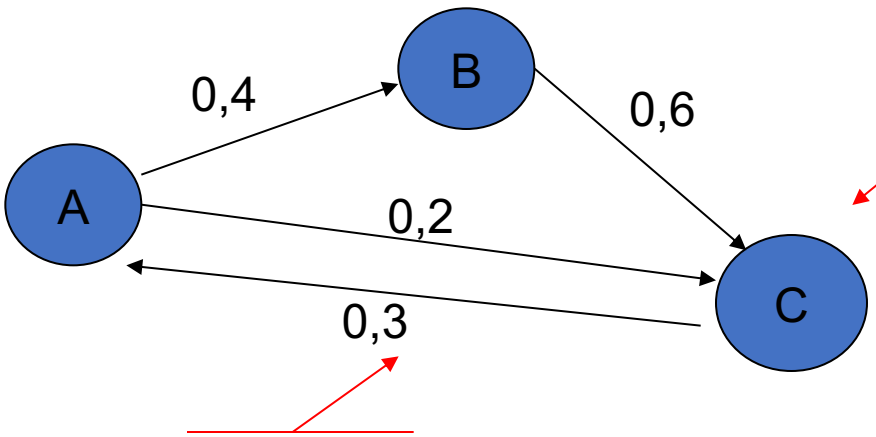
FORNITORI DI SERVIZI DI COMUNICAZIONE ELETTRONICA ACCESSIBILE AL PUBBLICO
OBBLIGHI IN MATERIA DI SICUREZZA (1 DI 3)

- Gli obblighi in materia di sicurezza e notifica degli incidenti per i **fornitori di servizi di comunicazione elettronica** prevedono che questi:

1) **adottino misure tecniche e organizzative adeguate al rischio esistente**, per salvaguardare la sicurezza dei propri servizi;
2) **garantiscano che i dati personali siano accessibili solamente al personale autorizzato** per fini legalmente autorizzati;
3) **garantiscano la protezione dei dati relativi al traffico e all'ubicazione e degli altri dati personali archiviati o trasmessi dalla distruzione accidentale, da perdita o alterazione anche accidentale e da archiviazione, trattamento, accesso o divulgazione non autorizzati, illeciti,** nonché assicurino l'attuazione di una politica di sicurezza;
4) **adottino**, congiuntamente con il fornitore della rete pubblica di comunicazioni, **le misure riguardanti la sicurezza della rete**, quando la sicurezza del servizio o dei dati personali richiedano anche l'adozione di misure che riguardano la rete stessa;
5) **informino i contraenti e, ove possibile, gli utenti, se sussiste un rischio di violazione della sicurezza della rete**, indicando, quando il rischio è al di fuori dell'ambito di applicazione delle misure, che il fornitore della rete stesso è tenuto ad adottare tutti i possibili rimedi ed i costi presumibili.

MODELLARE LE INTERDIPENDENZE

IIM



CI is an entity described by its inoperability level

Dependency (or Leontief) coefficient

u is external induced inoperability

$$\mathbf{x}(k+1) = \mathbf{R}\,\mathbf{x}(k) + \mathbf{B}\mathbf{u}$$

R is the interdependence matrix. Its entries represent the transmitted effects of inoperability

$r_{ii}=0$ if there is no recovery phenomena

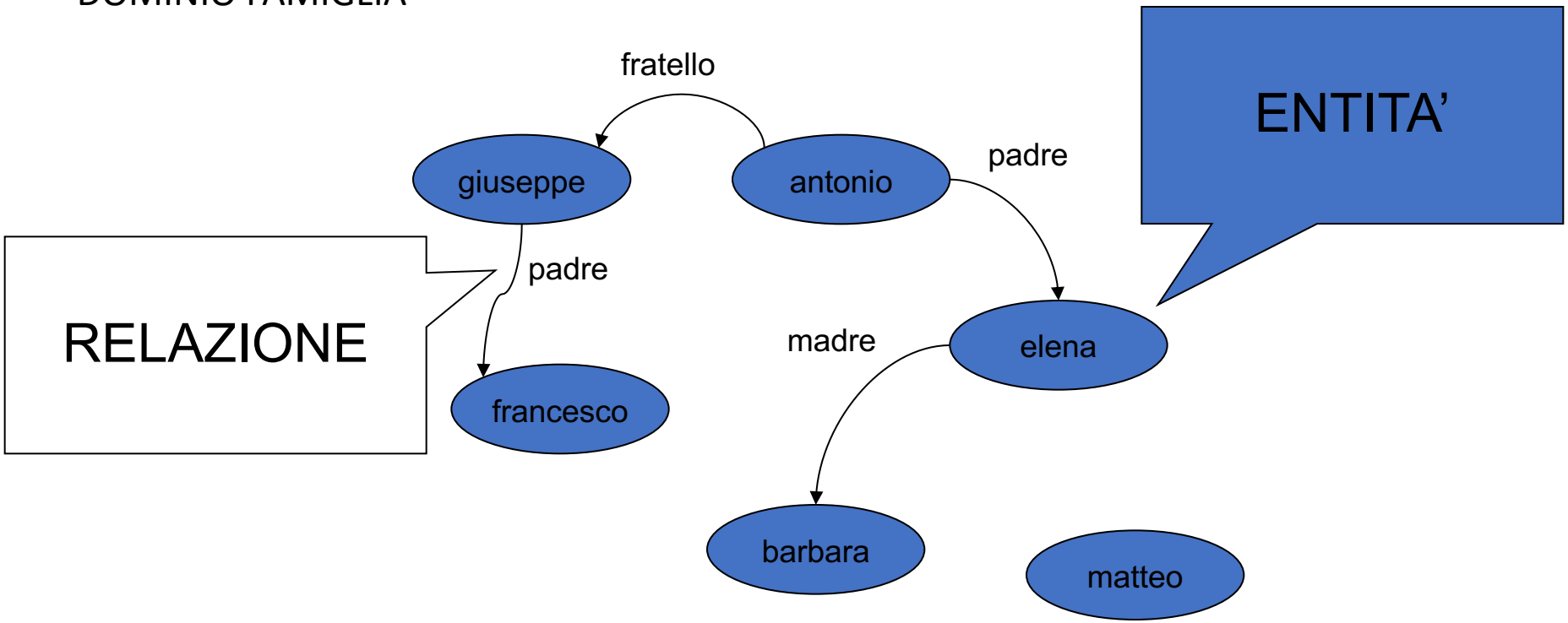
GENERALIZED STOCHASTIC PETRI NET

- Estensione probabilistica delle reti di Petri temporizzate
- Le variabili temporali associate alle transizioni sono variabili aleatorie

- Le attività il cui tempo di esecuzione può essere trascurato vengono modellate tramite transizioni istantanee

MODELLI ONTOLOGIGI

DOMINIO FAMIGLIA



Una ONTOLOGIA è caratterizzata da:

- un grafo orientato: i nodi rappresentano le entità, gli archi le relazioni
- un insieme di assiomi, vincoli e regole del dominio

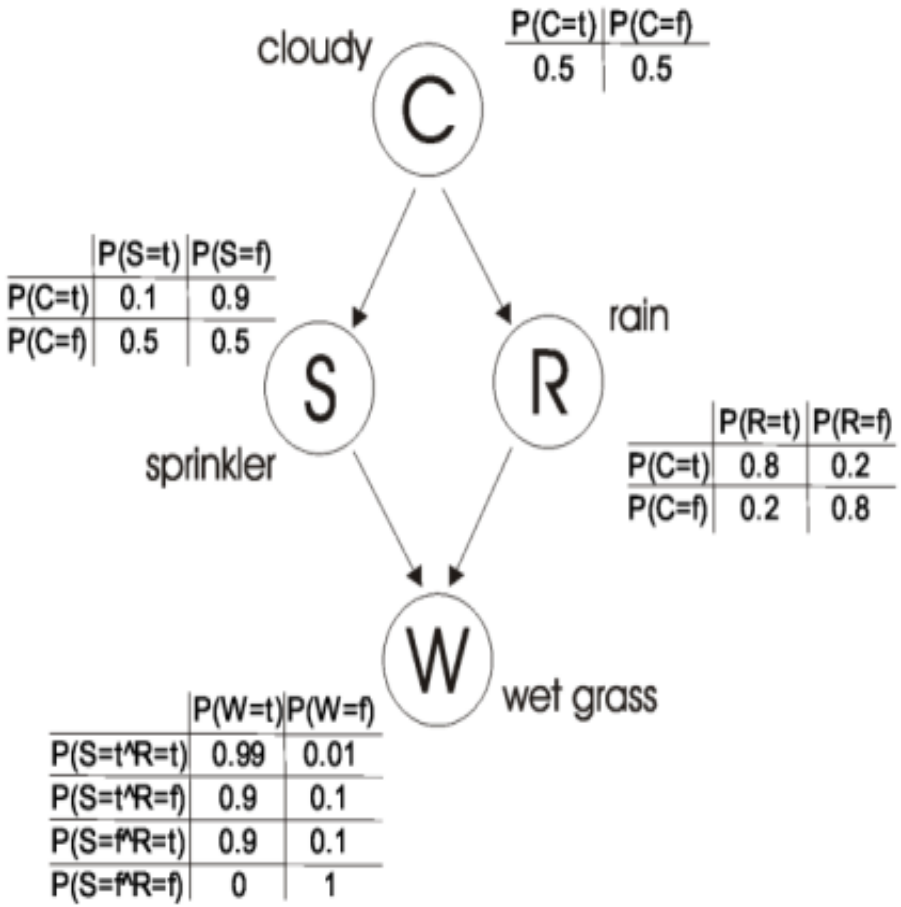
Bayesian Networks

The network is modeled with a **directed acyclic graph** of dependence structure between multiple interacting quantities where the **nodes represent random variables** and the <u>edges indicate conditional dependencies</u>.

For a directed model, we must specify the Conditional Probability Distribution at each node. To give an example, we consider only discrete variables in the following.

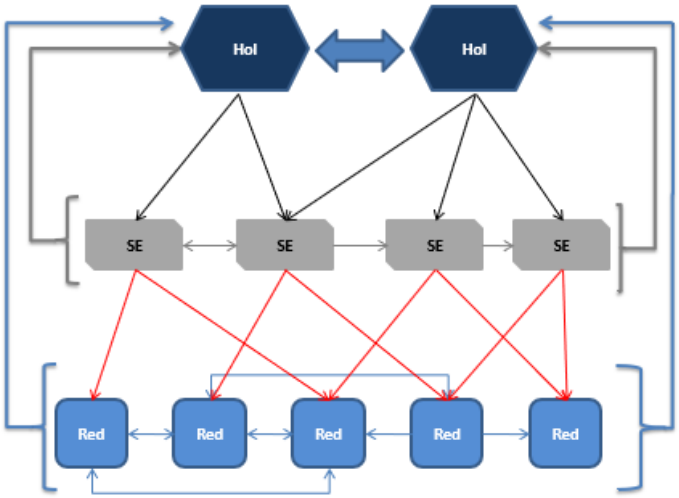
If the variables are discrete they can be represented as a table, which lists the probability that the child node takes on each of its different values for each combination of values of its parents.

Consider the following example, in which all nodes are binary, i.e., have two possible values, which are denoted by T (true) and F (false), respectively. The following graph shows the simple case for modeling the trivial example of a meadow.



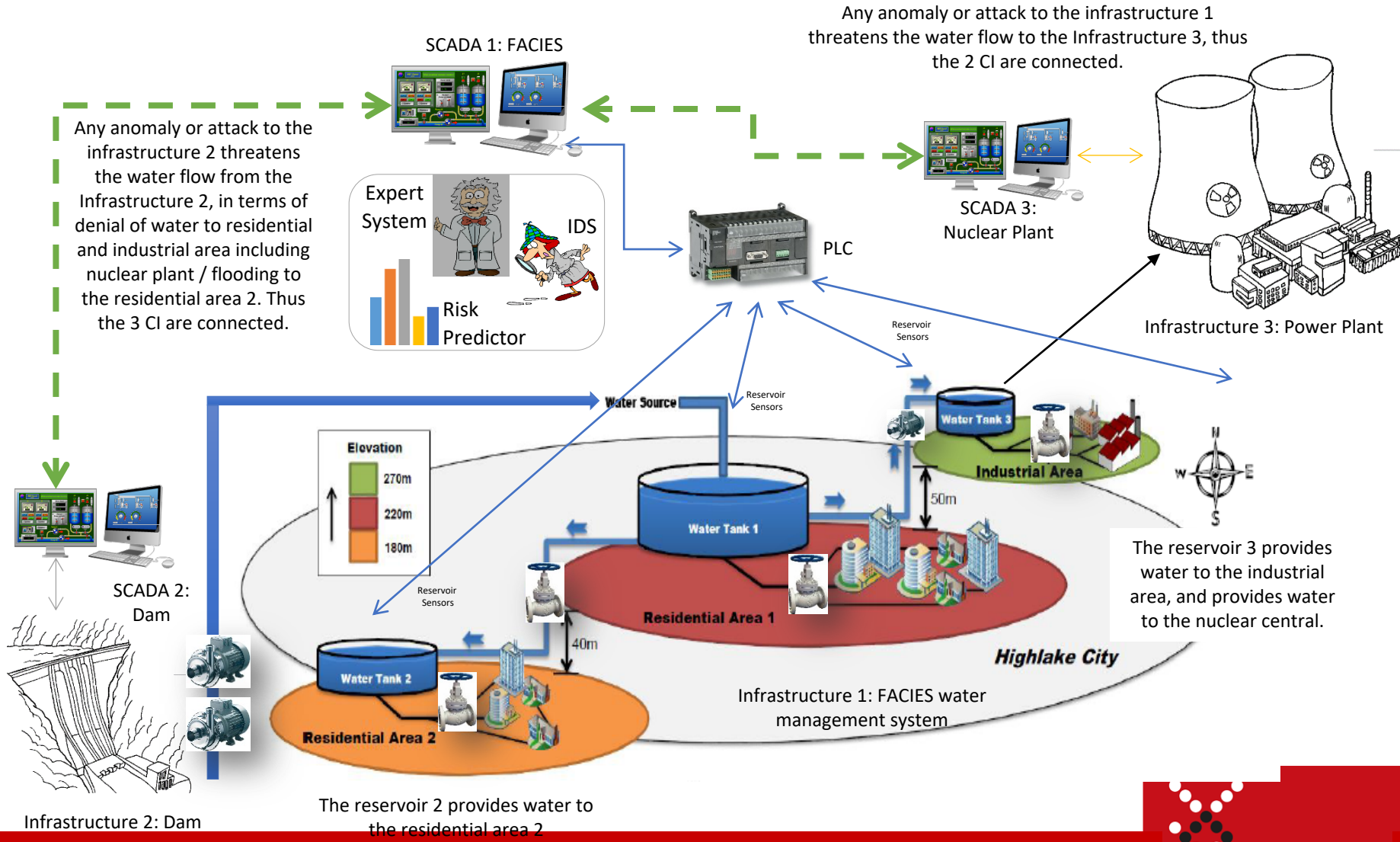
Agent Based Modeling Systems

- In ABMS a complex system is modeled as a set of interconnected, cooperative and or competitive interacting agents.
- An agent is an entity with a location, capabilities and memory.
- The entity location define where it is in a physical space (geographic region or abstract space, such as Internet).
- What the entity can perform is defined by its capabilities: perception, behaviors, intelligent reaction, cooperation and autonomy.
- Finally, the experience history (for example, overuse or aging) and data defining the entity state represent agent's memory.



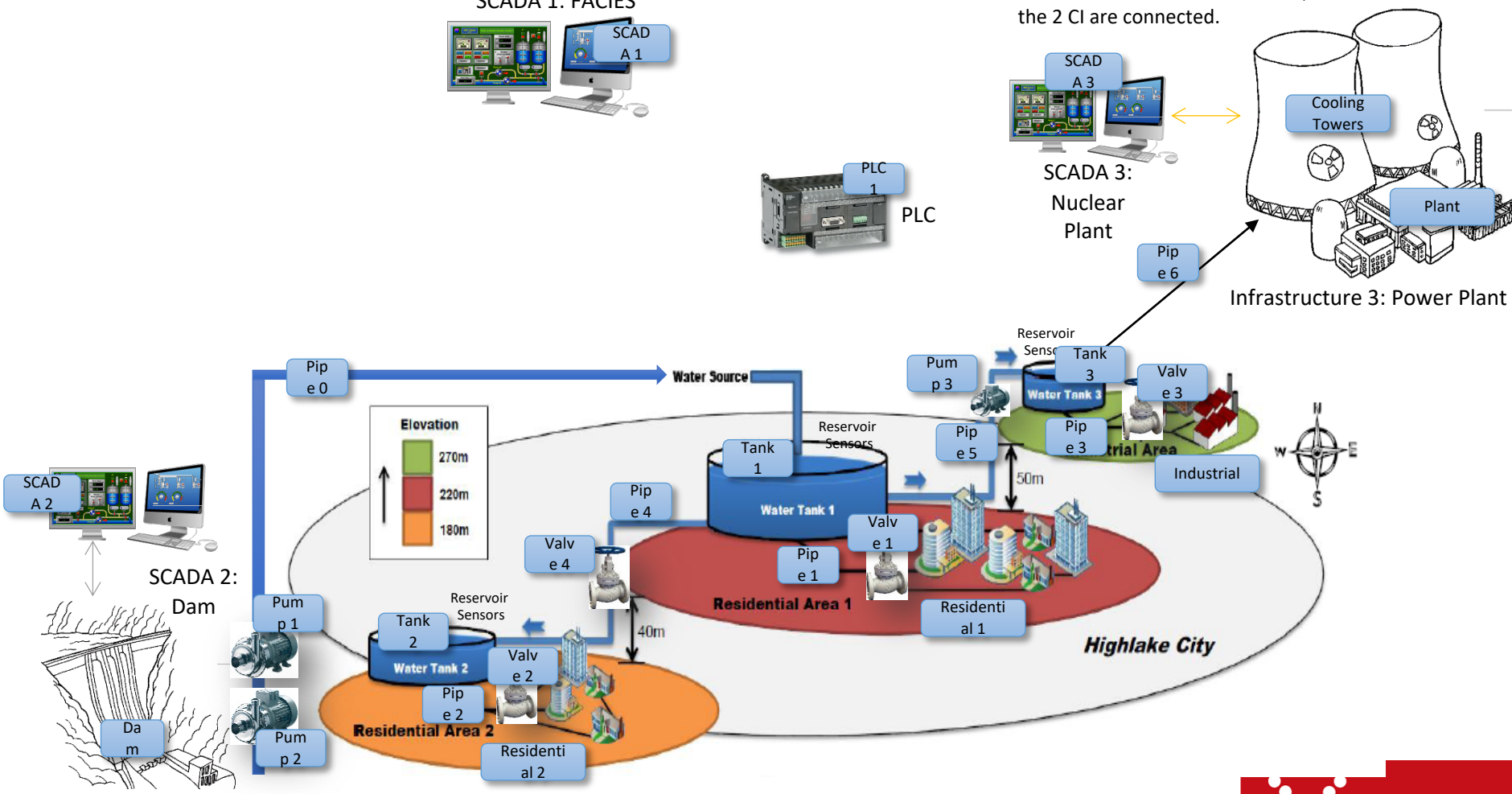
MHR Interdependency model

Multiple CI Interdependency Scenario

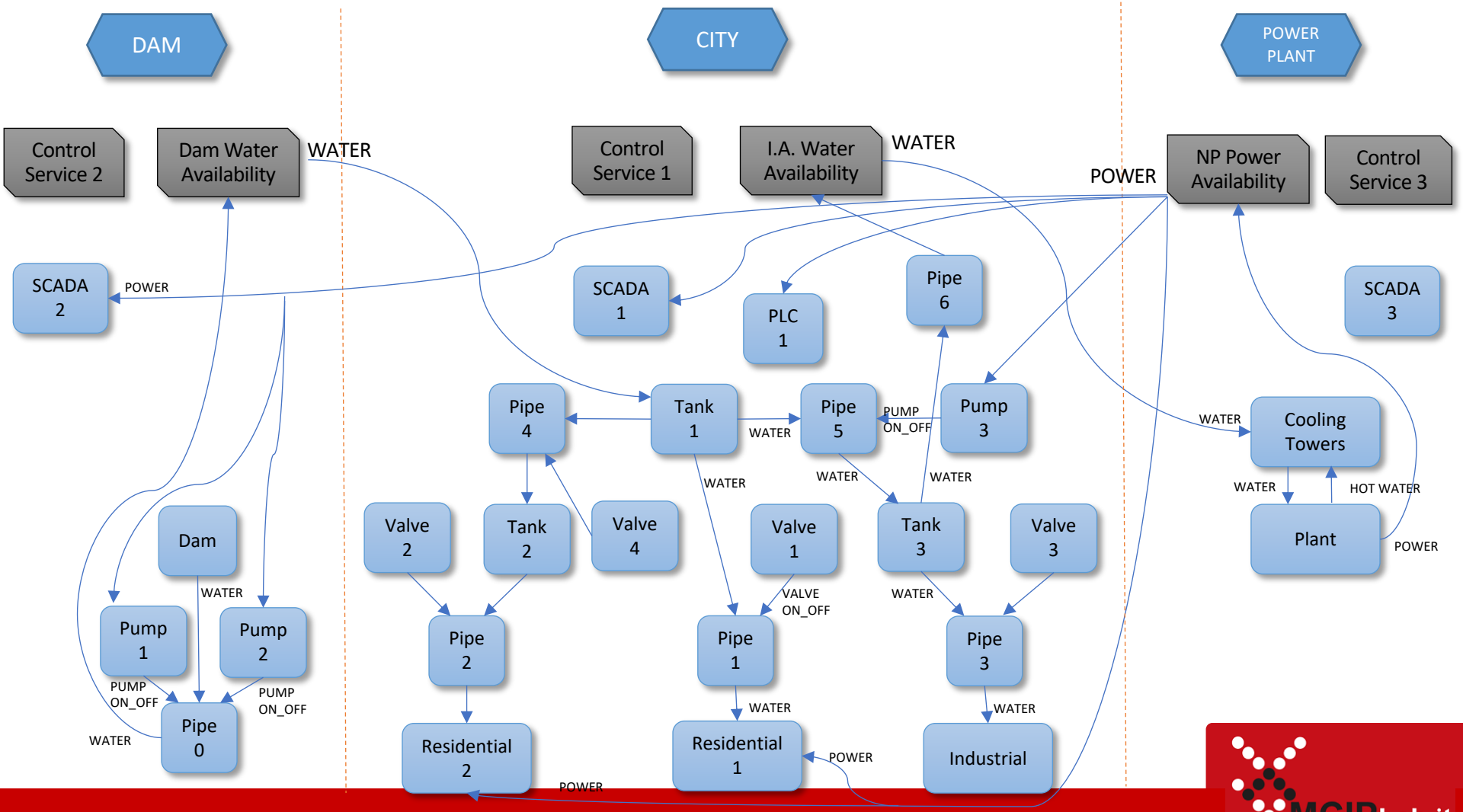


Elements of the Scenario

Any anomaly or attack to the infrastructure 1 threatens the water flow to the Infrastructure 3, thus the 2 CI are connected.



PHYSICAL DEPENDENCIES

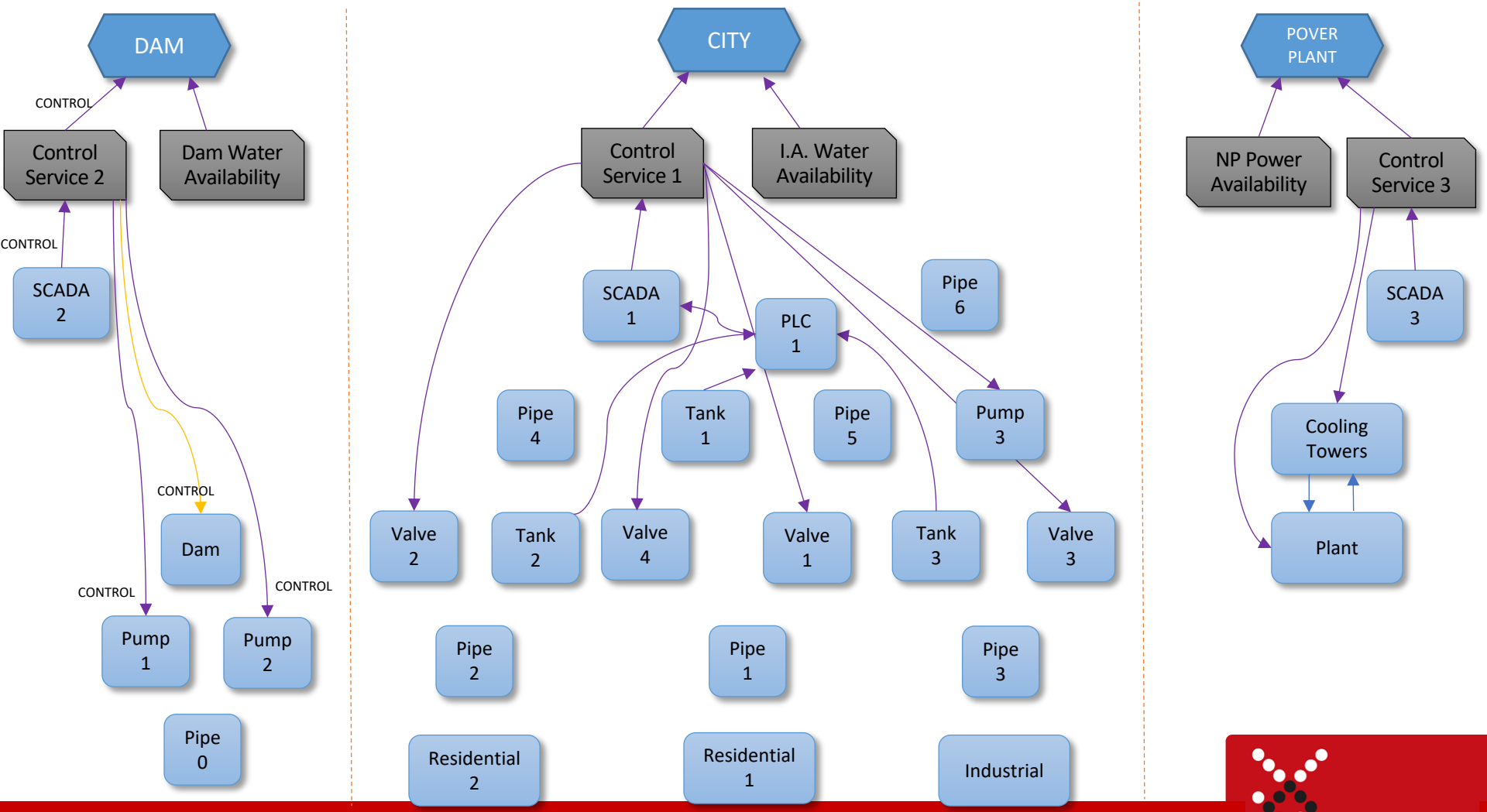


Physical Variables

- Element Services
- Water
- Power
- Hot_water
- Pump on_off
- Valve on_off

- Faults
- Mechanical
- Power lacking
- Plant warming
- Water supply (inverse logic)
- Power Supply (inverse logic)

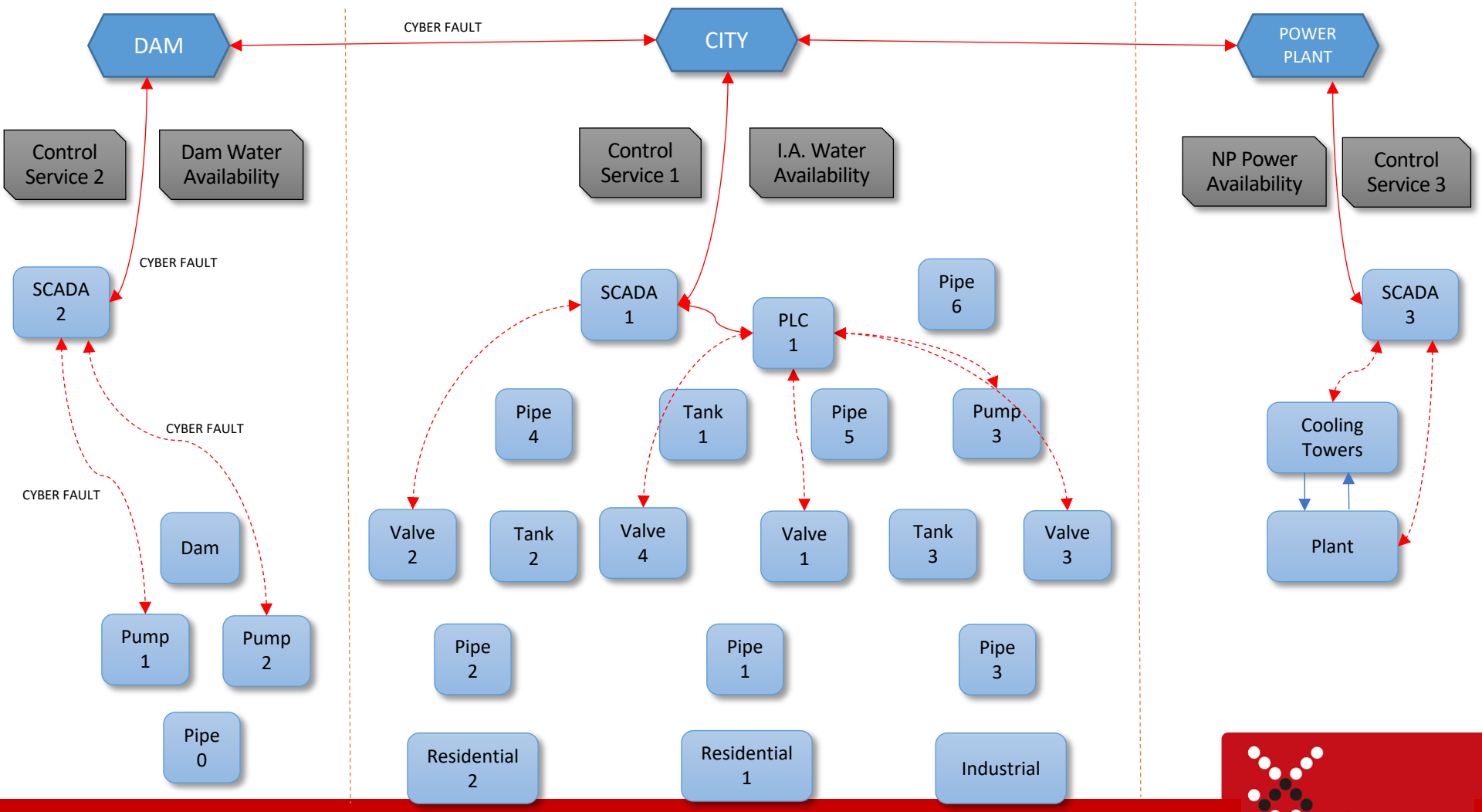
LOGICAL DEPENDENCIES



Logical Variables

- Element Services
- Control
- Faults
- Logical

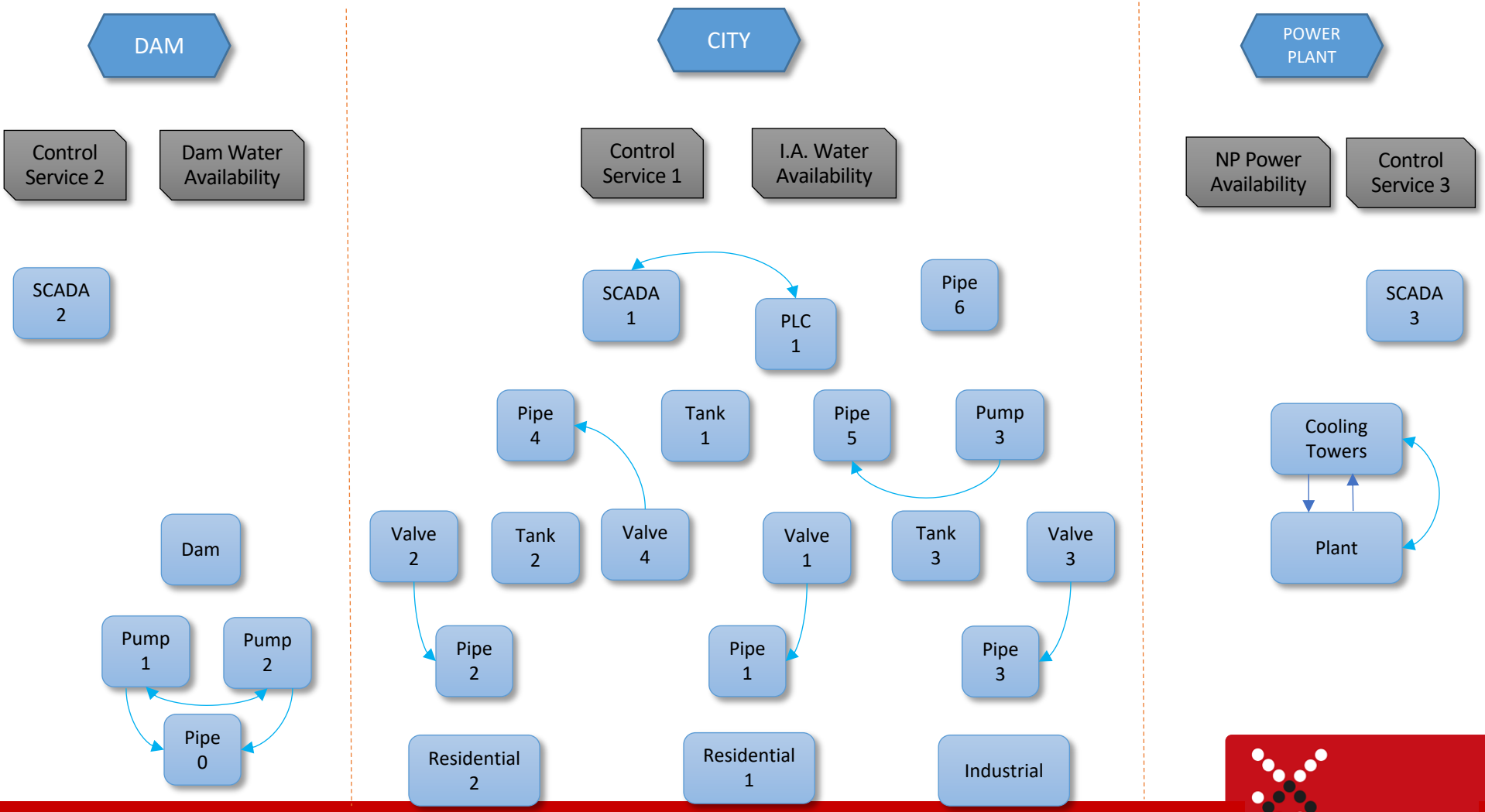
CYBER DEPENDENCIES



Cyber Variables

- Element Services
- Non infective
- Faults
- Cyber

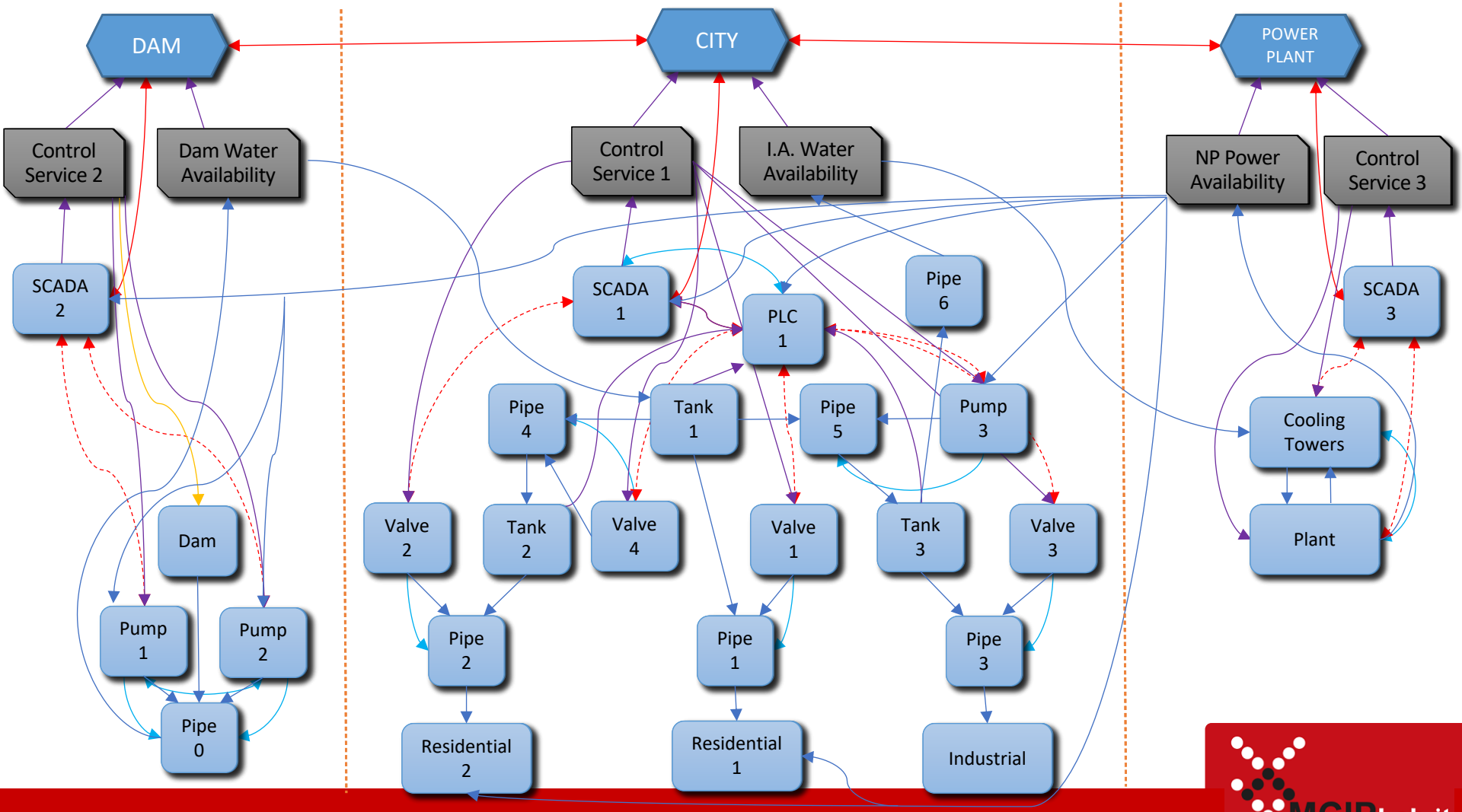
GEOGRAPHIC DEPENDENCIES



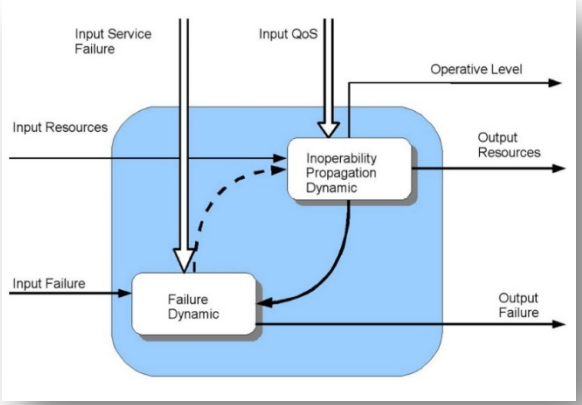
GEOGRAPHIC VARIABLES

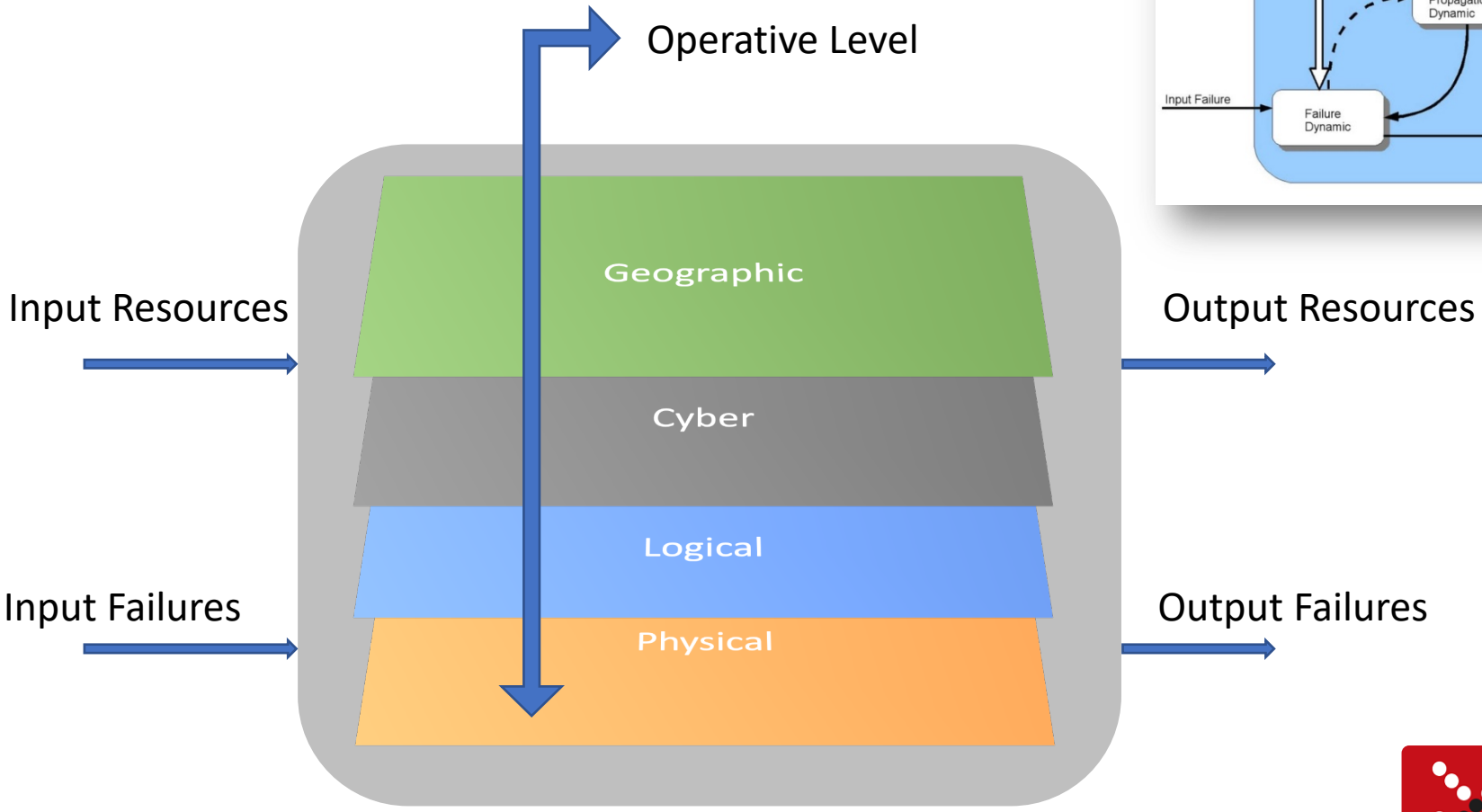
- Element Services
- <none>
- Faults
- Fire

All together



Operative Level



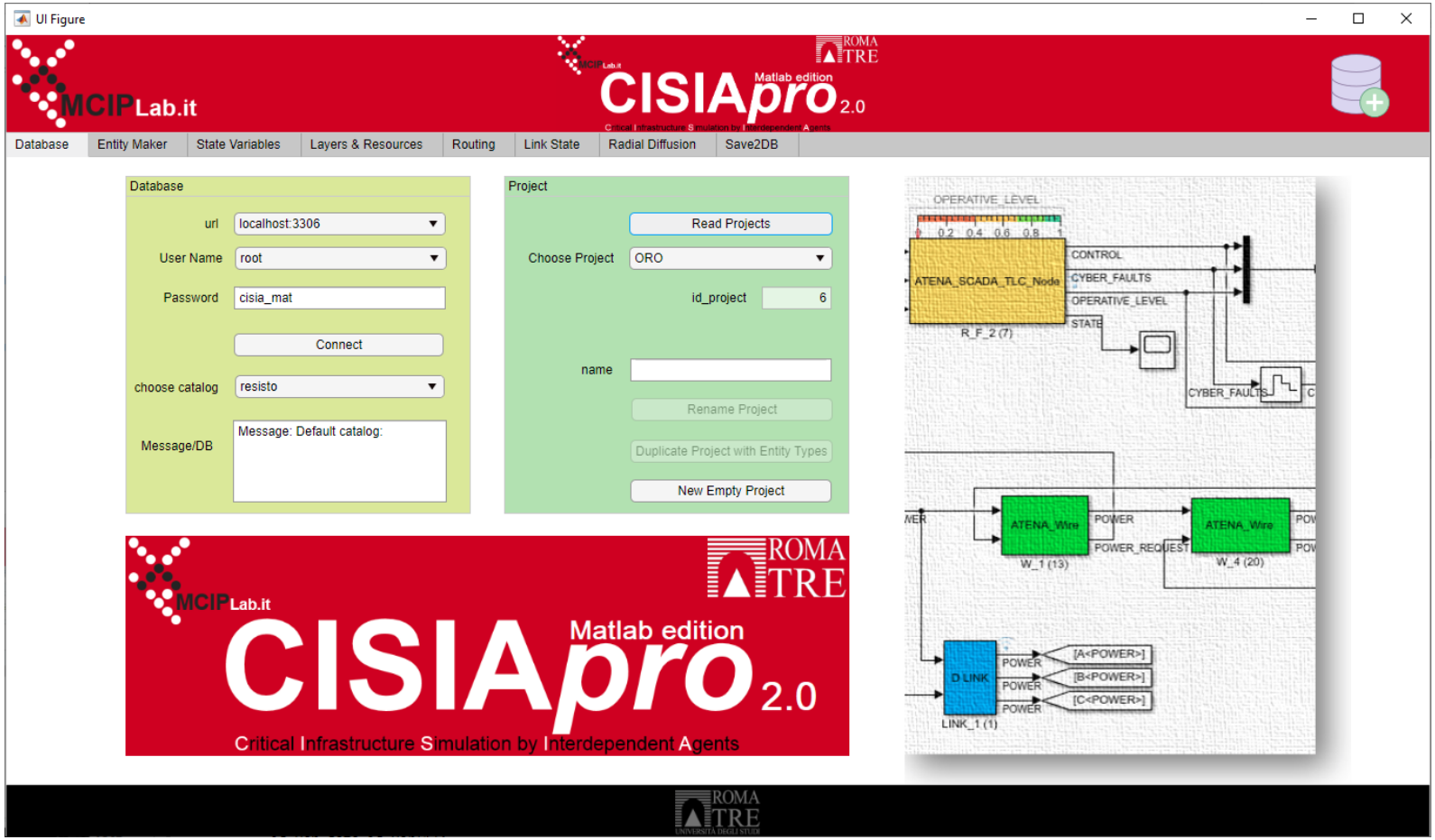


CISIApro 2.0

CISIAPRO V2.0

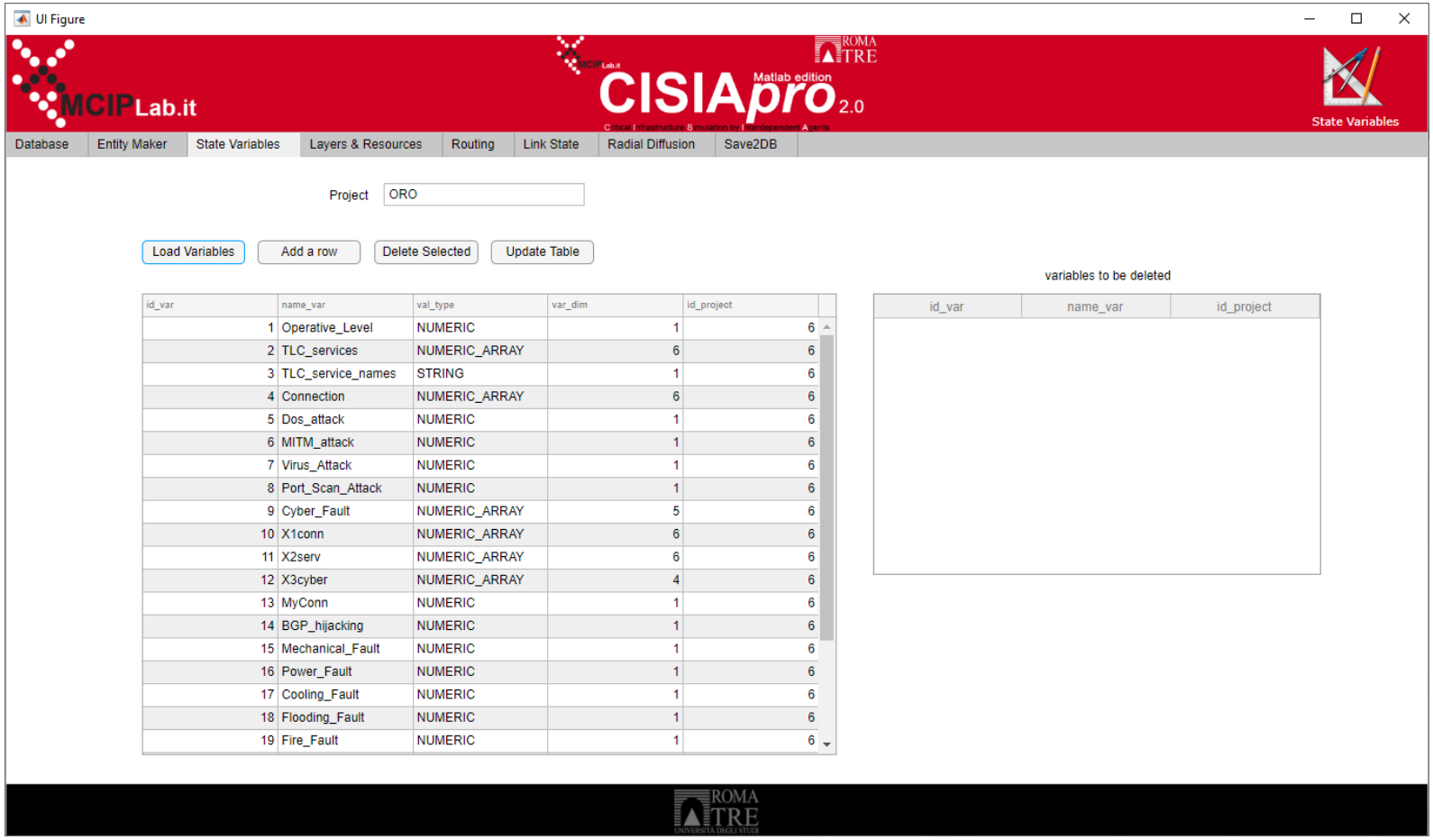
- A completely new and redesigned version of CISIApro has been completed to take into account some peculiar aspects of TLC networks
- In particular, have been introduced:
  - Dynamic links
  - Routing links
  - Propagation models for ring topologies
  - Continuous and discrete dynamics inside entities
  - The possibility of co-simulating external dynamics
  - A new tool for designing the whole system
  - A new user interface

CISIAPRO V2.0 MATLAB EDITION

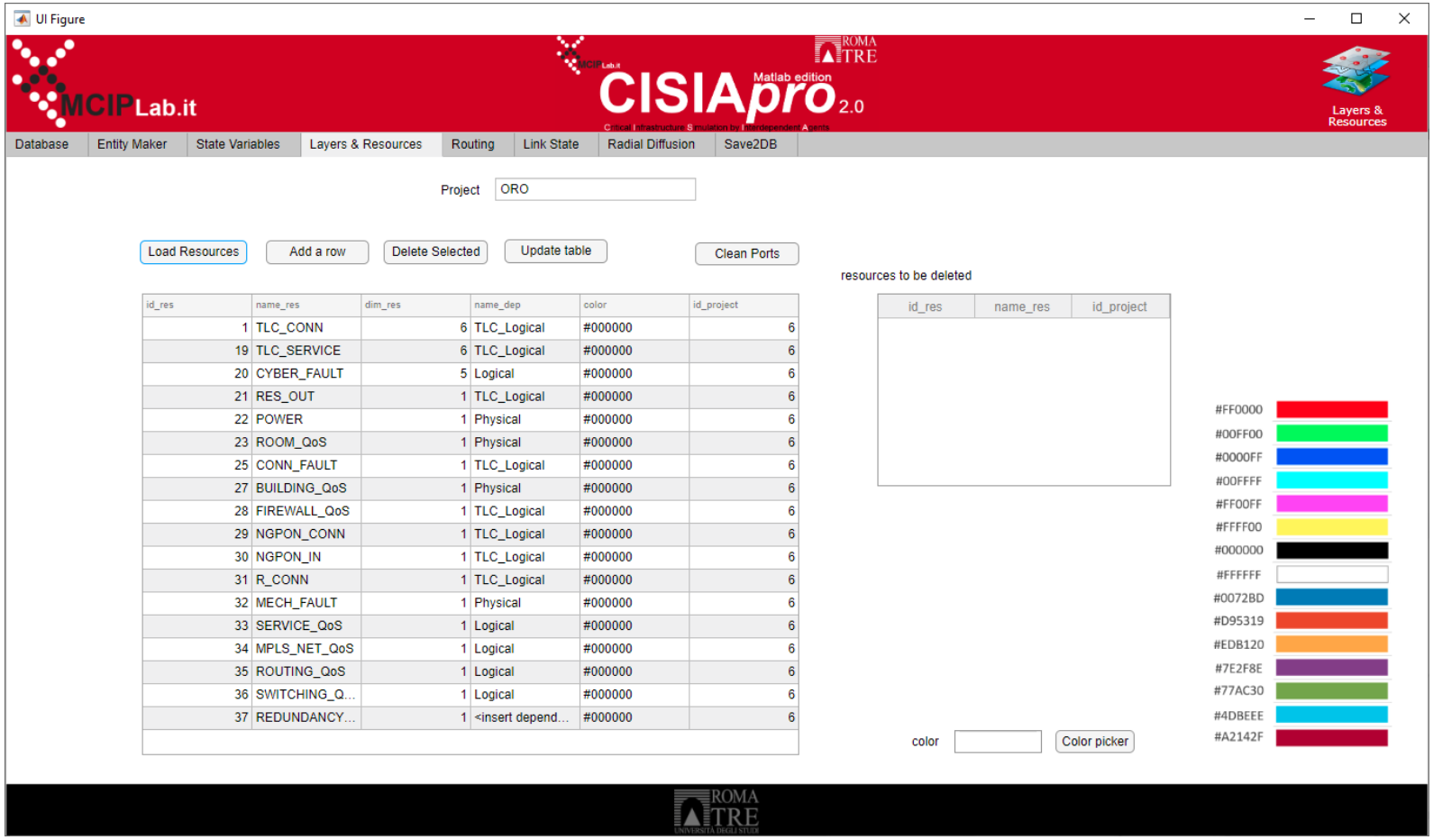


ENTITY MAKER

STATE VARIABLES

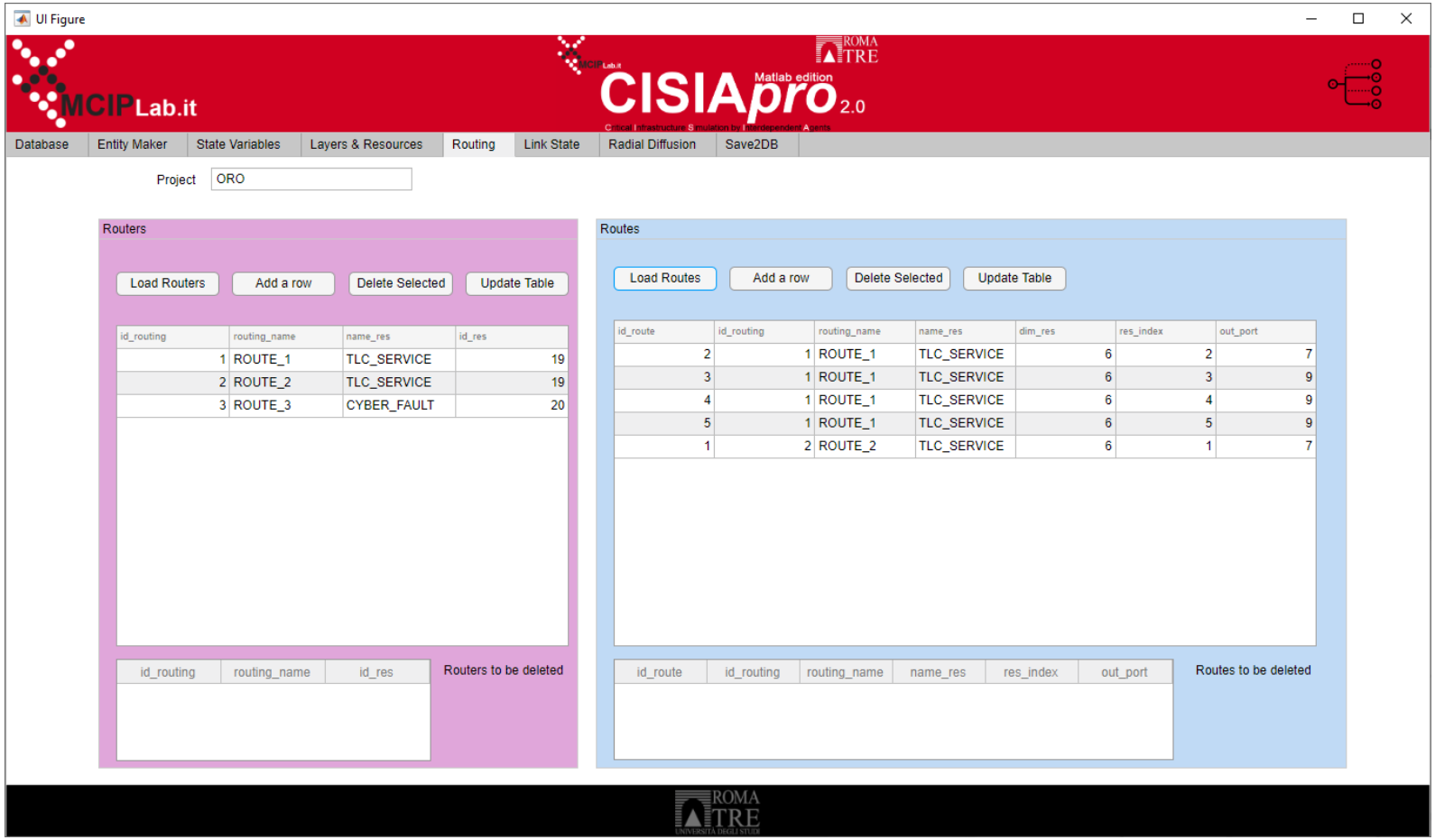


LAYERS & RESOURCES

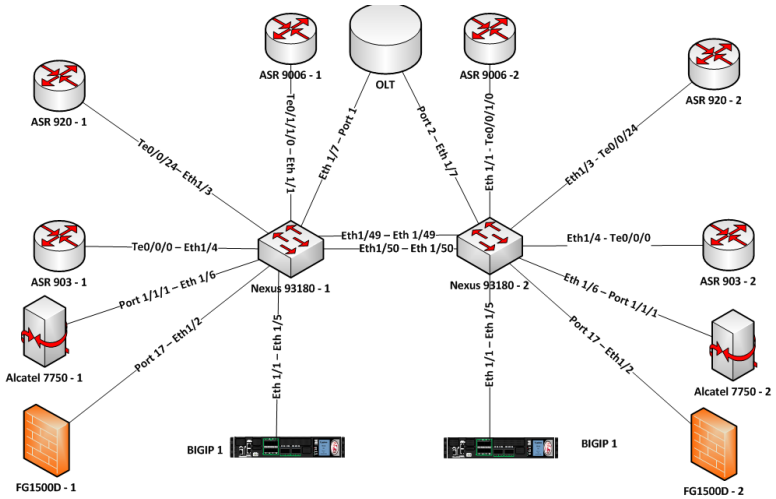


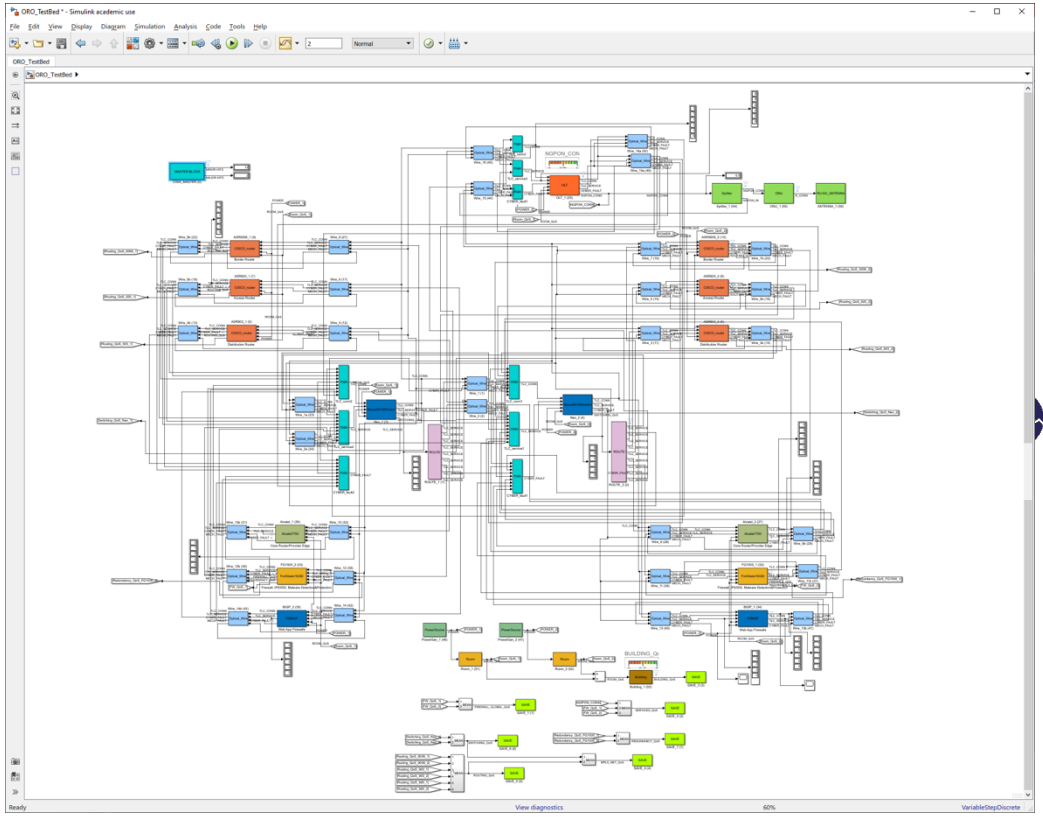
id_res	name_res	dim_res	name_dep	color	id_project
1	TLC_CONN	6	TLC_Logical	#000000	6
19	TLC_SERVICE	6	TLC_Logical	#000000	6
20	CYBER_FAULT	5	Logical	#000000	6
21	RES_OUT	1	TLC_Logical	#000000	6
22	POWER	1	Physical	#000000	6
23	ROOM_QoS	1	Physical	#000000	6
25	CONN_FAULT	1	TLC_Logical	#000000	6
27	BUILDING_QoS	1	Physical	#000000	6
28	FIREWALL_QoS	1	TLC_Logical	#000000	6
29	NGPON_CONN	1	TLC_Logical	#000000	6
30	NGPON_IN	1	TLC_Logical	#000000	6
31	R_CONN	1	TLC_Logical	#000000	6
32	MECH_FAULT	1	Physical	#000000	6
33	SERVICE_QoS	1	Logical	#000000	6
34	MPLS_NET_QoS	1	Logical	#000000	6
35	ROUTING_QoS	1	Logical	#000000	6
36	SWITCHING_Q...	1	Logical	#000000	6
37	REDUNDANCY...	1	<insert depend...	#000000	6

ROUTING

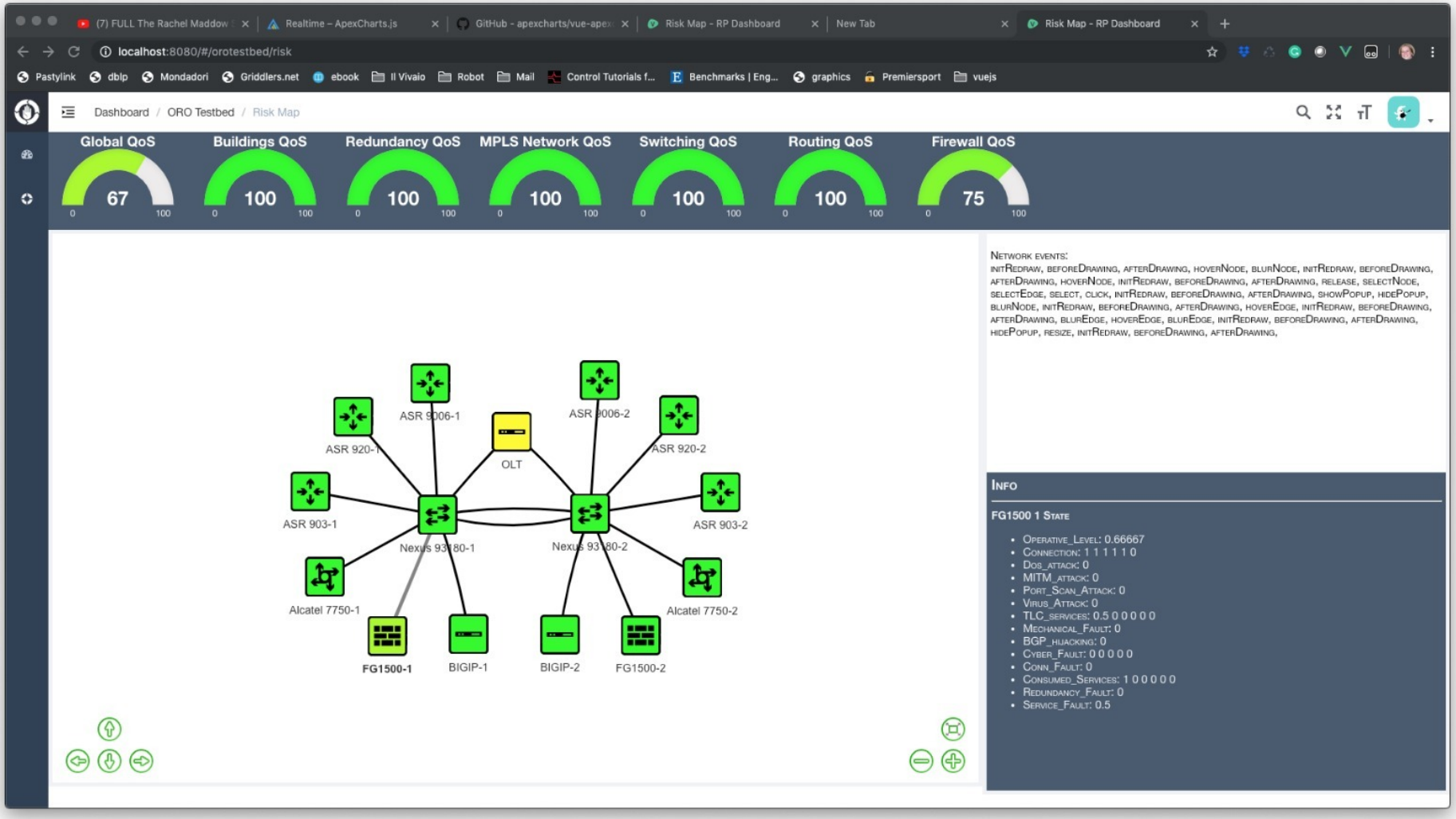

UI Figure
MCIPLab.it
CISIApro 2.0
Matlab edition
Database
Entity Maker
State Variables
Layers & Resources
Routing
Link State
Radial Diffusion
Save2DB
Project
ORO
Routers
Load Routers
Add a row
Delete Selected
Update Table
id_routing | routing_name | name_res | id_res
1 | ROUTE_1 | TLC_SERVICE | 19
2 | ROUTE_2 | TLC_SERVICE | 19
3 | ROUTE_3 | CYBER_FAULT | 20
id_routing | routing_name | id_res
Routers to be deleted
Routes
Load Routes
Add a row
Delete Selected
Update Table
id_route | id_routing | routing_name | name_res | dim_res | res_index | out_port
2 | 1 | ROUTE_1 | TLC_SERVICE | 6 | 2 | 7
3 | 1 | ROUTE_1 | TLC_SERVICE | 6 | 3 | 9
4 | 1 | ROUTE_1 | TLC_SERVICE | 6 | 4 | 9
5 | 1 | ROUTE_1 | TLC_SERVICE | 6 | 5 | 9
1 | 2 | ROUTE_2 | TLC_SERVICE | 6 | 1 | 7
id_route | id_routing | routing_name | name_res | res_index | out_port
Routes to be deleted

CISIAPRO 2.0 PROPAGATION MODEL





New User Interface



A real-time propagation-based approach to risk evaluation

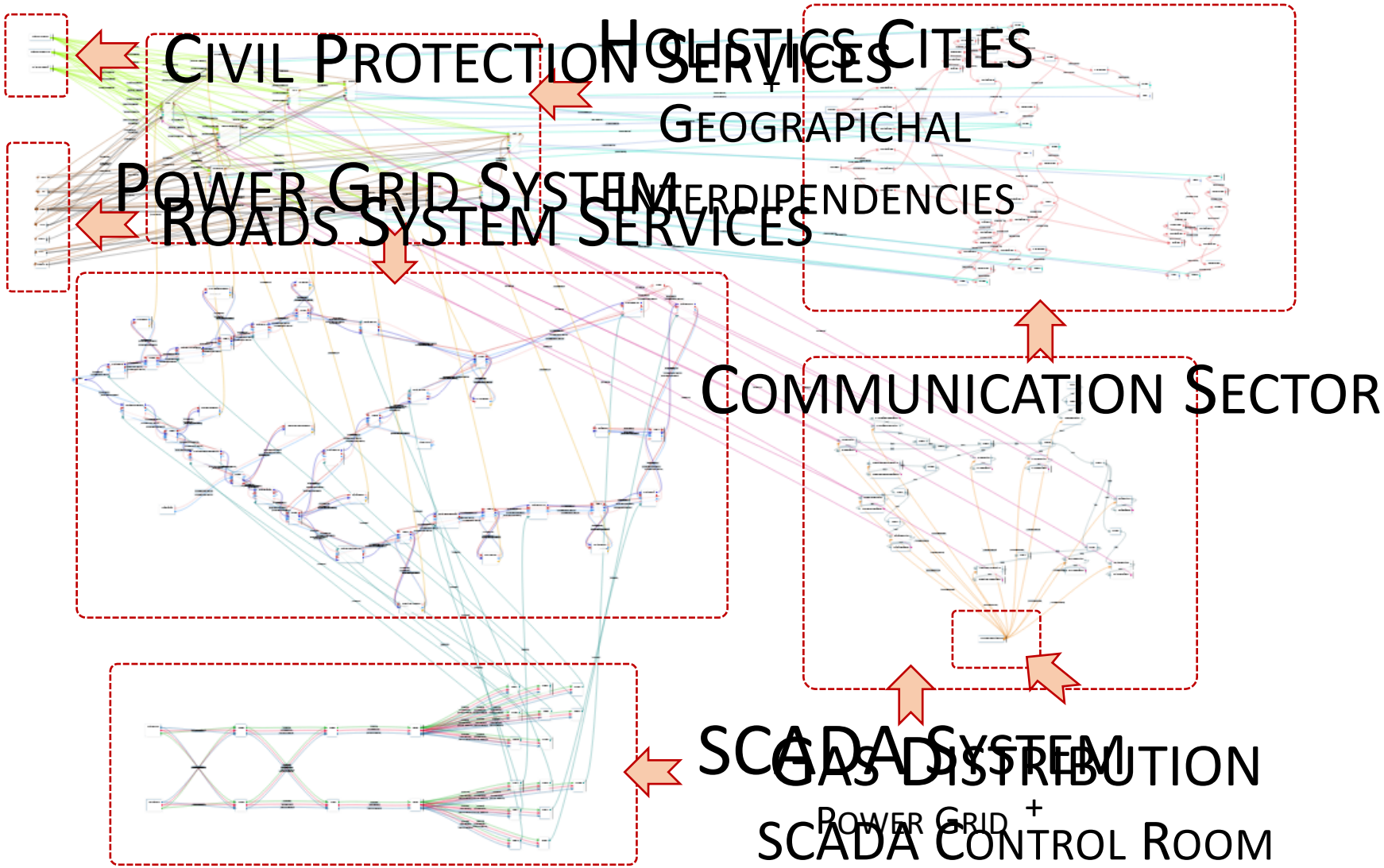
1 - Definition of a Reference Scenario

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

- System of Systems
  - Critical Infrastructures (water, gas, transports, power, finance, politics, research)
  - Industrial Assets
  - Cultural Assets
  - Touristic Assets
- Decomposition in elementary subsystems
- Definition of dependencies and interdependencies

MCIPLab.it

MHR modelling (CISIAPro 1.0)



2 - Hazards analysis

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

- Which are the negative events that we want to consider?
- Which are the immediate effects of such events?
- Which elements will be completely or partially damaged?
- In this phase we have to make the vulnerability assessment

- Examples
  - Fire
  - Flooding
  - Plant incident
  - Explosion
  - Train derailment
  - Cyber-attack
- But also
  - A bomblet during a football match
  - An incident during an event
  - Water Contamination
- And more
  - Adverse Weather events
  - Seismic events
  - Large Flooding
  - Eclipses
  - Windstorm

MCIPLab.it

3 - Key Process Definition

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

- What we need to protect?
- Is there a complex system whose risk we want to define?
- Which vital process risk we want to evaluate?
- Which activity we want to help with additional situational awareness?

- Examples
  - The possibility of reconfiguring a physical asset (Electricity, GAS, …) to recover from a fault
  - The energy balancing process at regional level
  - Increase the awareness of a civil protection control room

MCIPLab.it

4 -Define input data

- Traditional control rooms
  - SCADA systems
  - Fire brigades
  - Police
  - Civil Protection
- Physical alarms
- Weather data
- Seismic data
- Cyber information
  - Infrastructures' IDS
  - CERT
- Any other sensor network deployed in the field
- Crowdsourcing

VERSO UN DECISION SUPPORT SYSTEM

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

1. Detection → Sensors detect abnormal behavior
2. Threat Assessment → Type of alarm recognition and damage level definition and local risk
3. CISIApro → Variables propagation effects
4. DSS → Operational actions against crisis
5. Operative suggestions

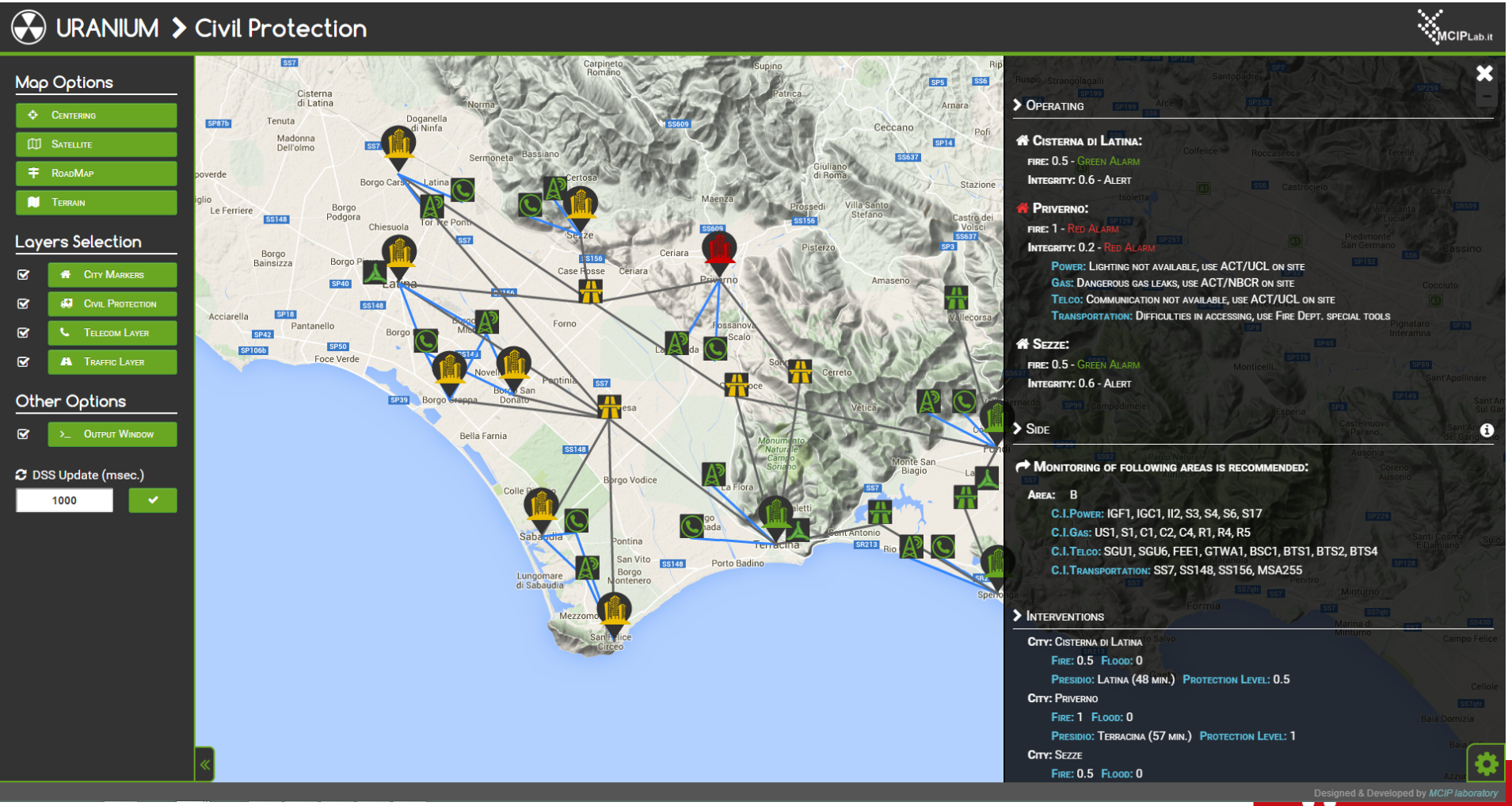
Situation Assessment & Risk Evaluation

MCIPLab.it

CONSOLE

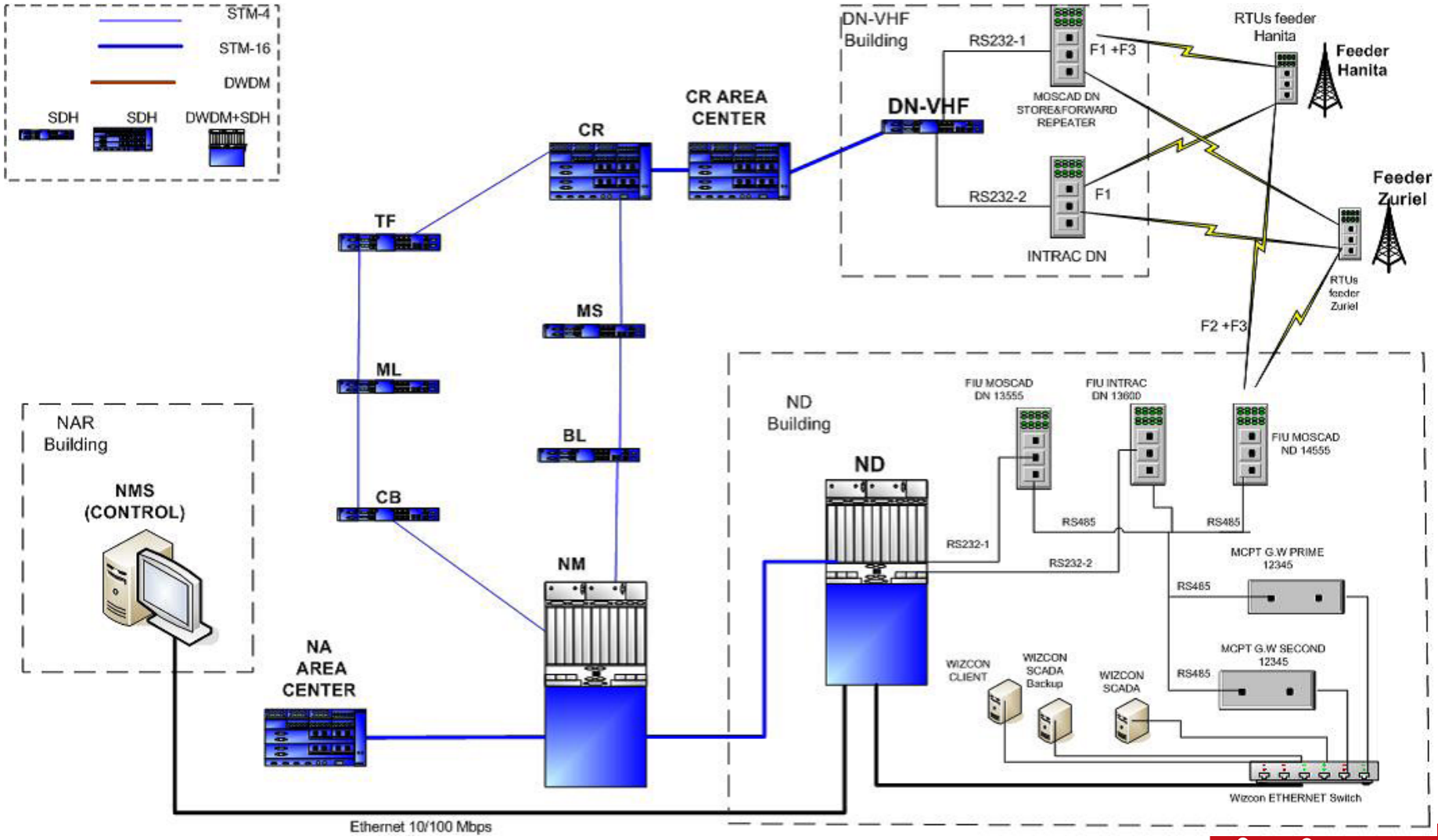
ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

CISIApro and DSS HMI



MCIPLab.it

CYBER-CASCADING EFFECTS



MCIPLab.it

ROMA TRE

CISIApro 2.0

Matlab edition

Critical Infrastructure Simulation by Interdependent Agents

Thanks

panzieri@uniroma3.it