

EDUCATION AND TRAINING

## CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

### Next level cybersecurity education and training



Co-funded by  
the European Union

# Effetti a cascata nelle reti sanitarie complesse

## CSP008\_S\_H

PRESENTAZIONE DA PARTE DI:  
DR. STEFAN SCHAUER  
DR. ABDELKADER SHAABAN  
AIT ISTITUTO AUSTRIACO DI TECNOLOGIA

EDUCATION AND TRAINING

# CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

## Next level cybersecurity education and training



Co-funded by  
the European Union

# Riconoscimento

- *Co-finanziato dall'Unione Europea. I punti di vista e le opinioni espresse sono tuttavia esclusivamente quelli dell'autore o degli autori e non riflettono necessariamente quelli dell'Unione Europea o di HADEA. Né l'Unione Europea né l'autorità che ha concesso il finanziamento possono essere ritenute responsabili.*
- *Accordo di progetto n. 101083594*

# Effetti a cascata nelle reti sanitarie complesse

## Panoramica

- Argomento-1: Introduzione alle infrastrutture critiche
- Argomento-2: Il panorama delle minacce nel settore sanitario
- Argomento 3: Interdipendenza delle infrastrutture critiche
- Argomento 4: Effetti a cascata e loro impatto
- Argomento 5: Simulazione e analisi degli effetti a cascata

# Ordine del giorno

- o1. Entità critiche
- o2. Interdipendenze Effetti a cascata
- o3.

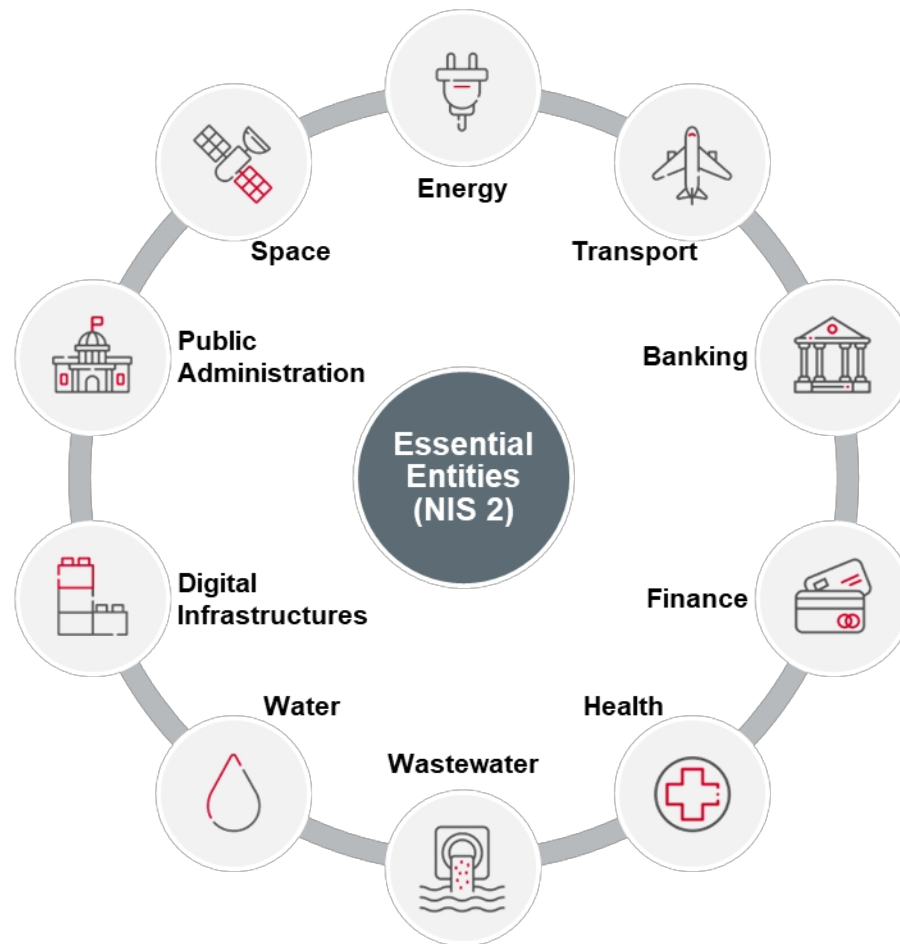
# Entità critiche

Cosa sono le infrastrutture critiche e  
gli asset critici presenti?

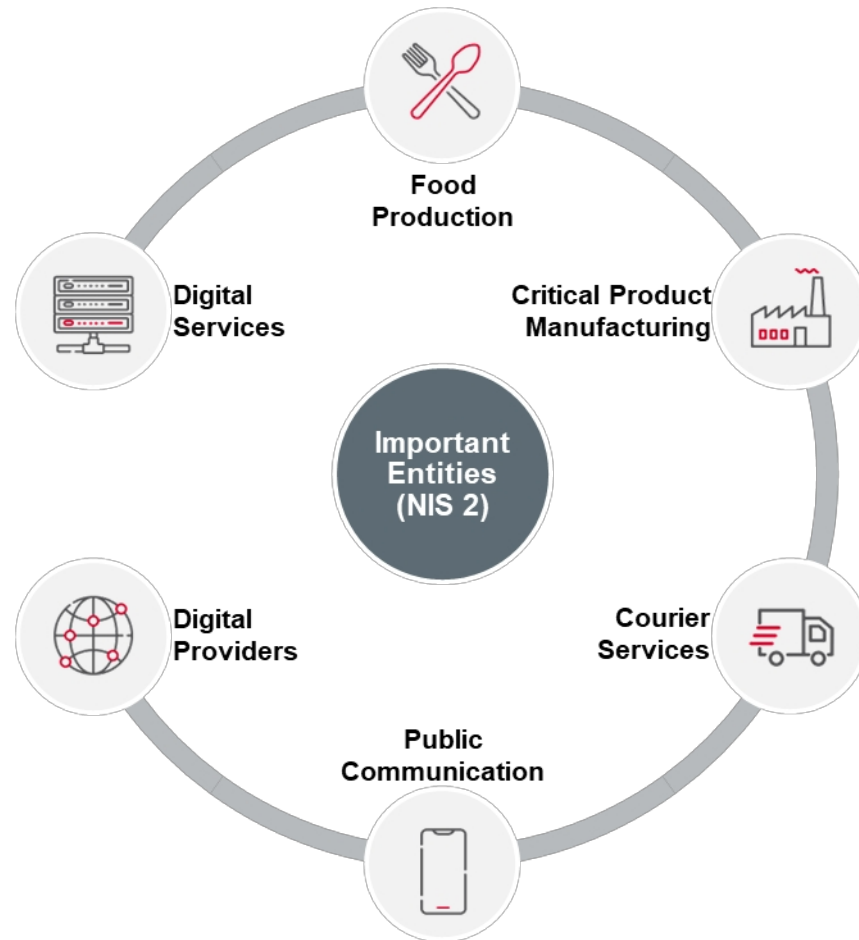
# Infrastrutture critiche

- Le infrastrutture critiche (IC) sono fondamentali per il **mantenimento delle funzioni vitali della società**
  - **Reti di base della catena di approvvigionamento** (elettricità, gas, acqua)
  - **Reti di informazione e comunicazione (TIC)**
  - Sistemi complessi ad **alto impatto sociale** ( mediche, finanza, reti di trasporto)

# Infrastrutture critiche



# Infrastrutture critiche



# Infrastrutture critiche



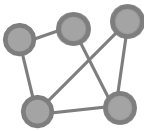
Fornitura di cibo



Trasporto



Ospedale



Rete del gas



Centrale elettrica



Governo



Raffineria



Porto di mare

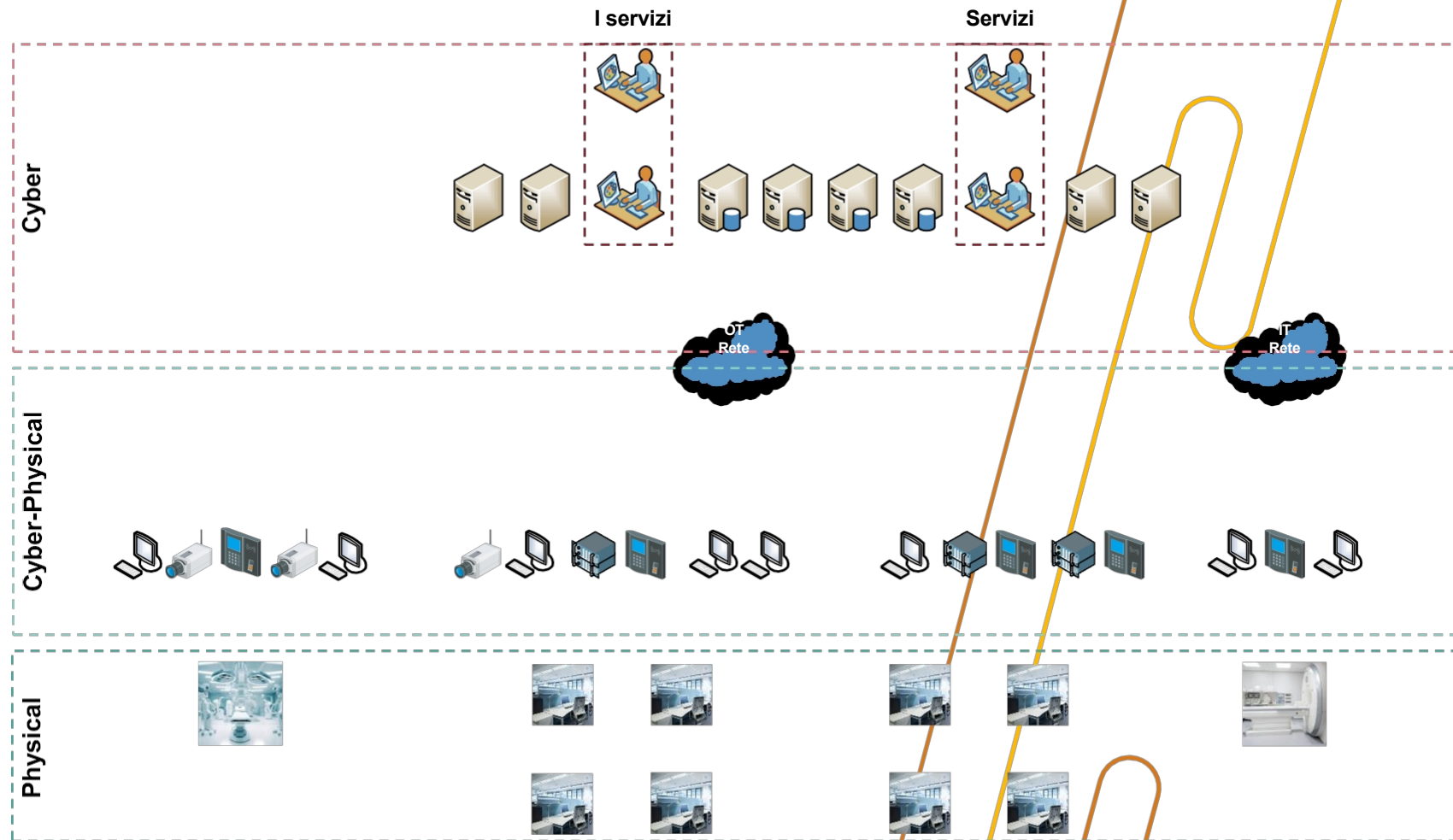


Finanza

# Attività critiche

- All'interno delle infrastrutture critiche o delle organizzazioni in generale **gli asset o i componenti critici** possono essere definiti
  - Fornire **funzionalità di base** per l'organizzazione
  - Necessario per **mantenere il servizio** dell'organizzazione
- Tali asset o componenti critici possono essere situati in **diversi domini**
  - **Fisico**: parti essenziali della rete di distribuzione (pompe, sottostazioni, tubazioni, ecc.).
  - **Cyber-Fisica**: sistemi di monitoraggio e controllo (PLC, sensori, interruttori, ecc.)
  - **Cyber**: infrastruttura virtuale e software (server, database, applicazioni)

# Attività critiche

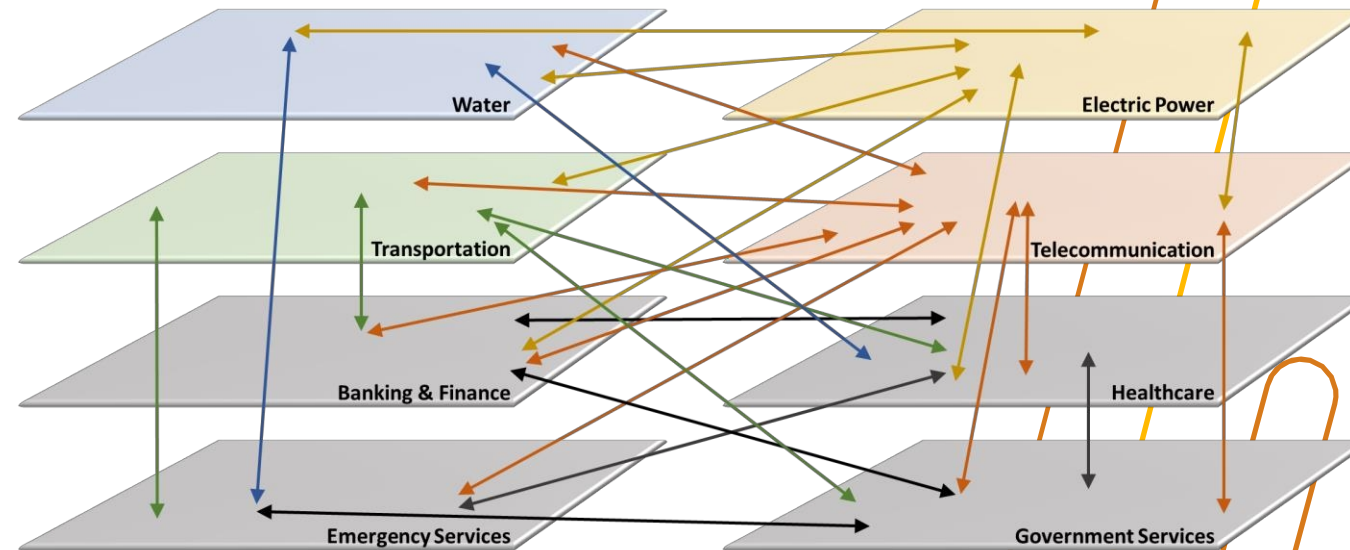


# Interdipendenze

Come possono le dipendenze tra  
Le entità critiche devono essere caratterizzate?

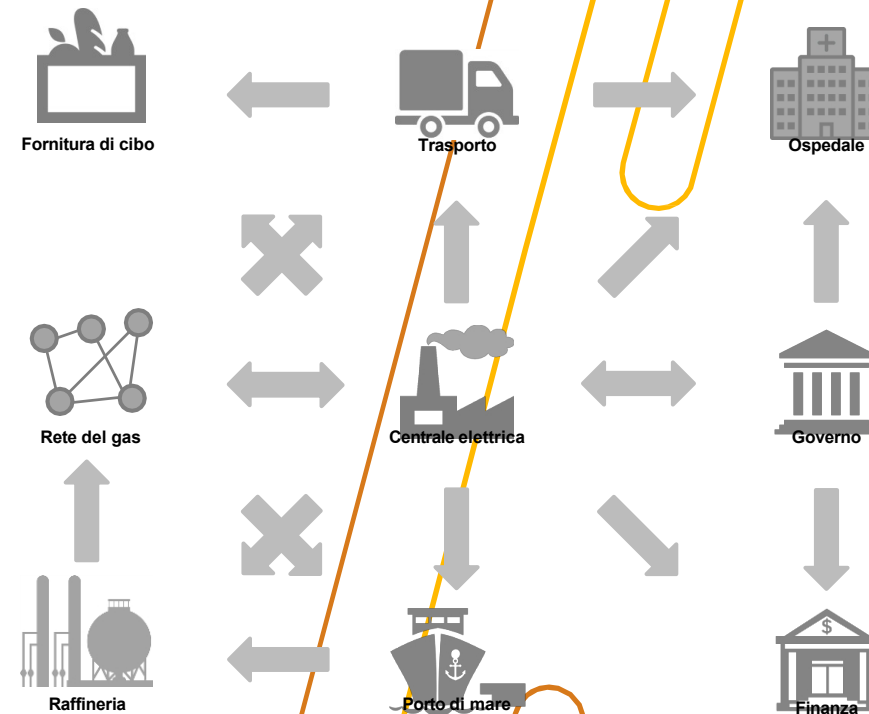
# Interdipendenze dell'infrastruttura

- Negli ultimi decenni le entità critiche sono diventate sempre più **interrelati e interdipendenti**
- Relazioni complesse tra **fornitori di servizi e consumatori**
- **Catene di approvvigionamento** intrecciate e spesso **fragili** su scala nazionale e internazionale



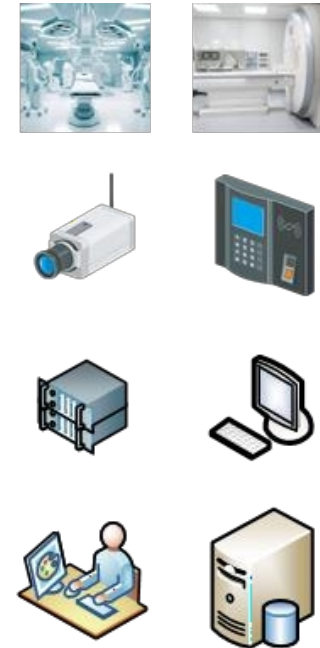
# Interdipendenze dell'infrastruttura

- Le infrastrutture critiche non possono essere considerato in modo isolato
- Le infrastrutture agiscono come fornitori di **diverse risorse e servizi**.
- Le infrastrutture agiscono anche come **consumatori** di alcune **risorse e servizi** di altre infrastrutture per garantire la funzionalità.

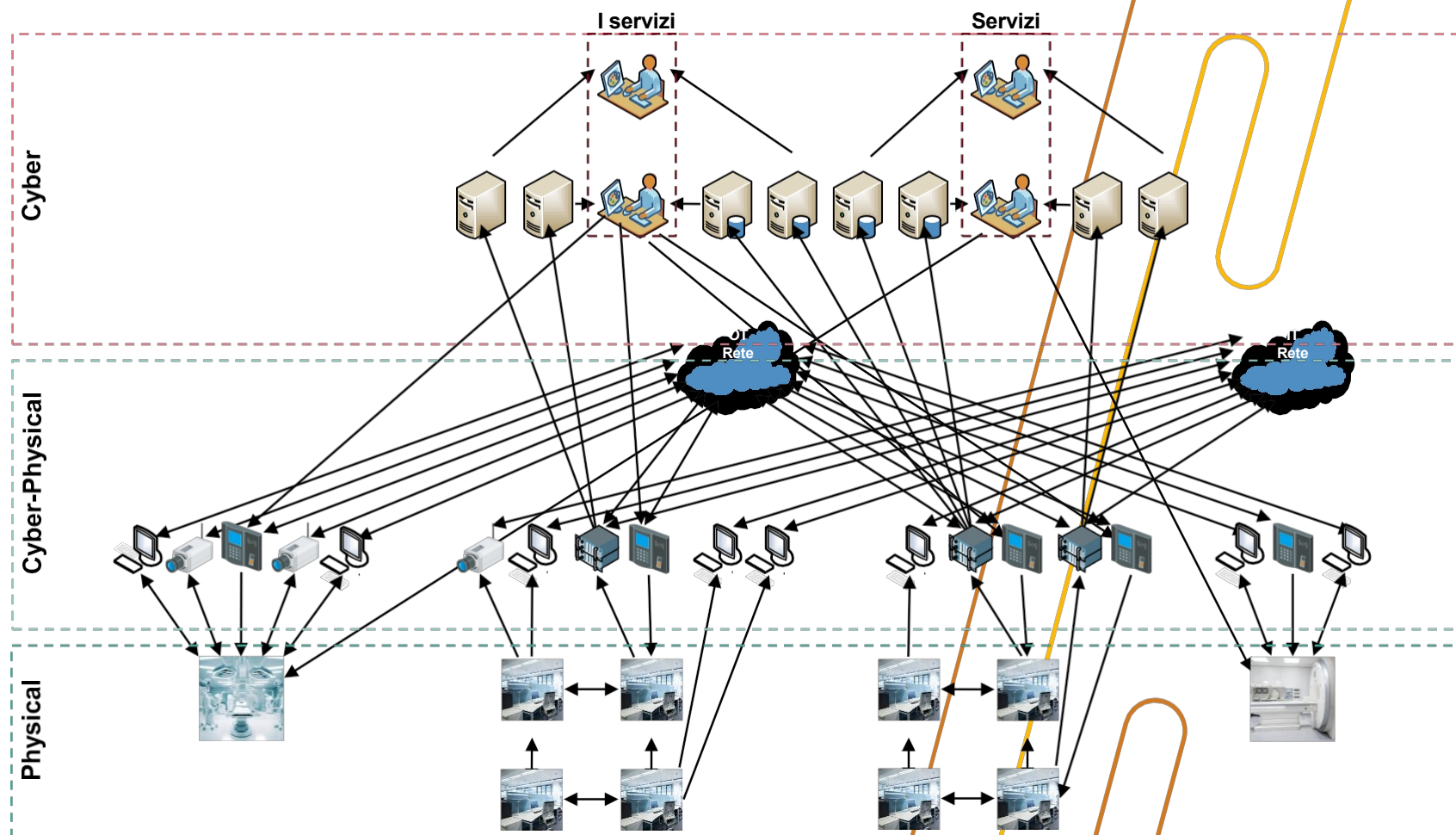


# Interdipendenze dell'infrastruttura

- Le interdipendenze esistono anche **all'interno delle organizzazioni e tra le organizzazioni stesse. i loro locali**  
a causa dell'**aumento della digitalizzazione e dello scambio di dati**
  - **Gli edifici e i macchinari** sono "intelligenti" e sono collegati a sistemi digitali
  - Sistemi di **videosorveglianza e controllo accessi** può influenzare gli asset fisici
  - **I sensori e i dispositivi dell'Internet of Things (IoT)** collegano le risorse fisiche e informatiche.
  - **I servizi** sono forniti da **applicazioni** in esecuzione su server reali o virtuali.
- La funzionalità e i servizi di un'infrastruttura possono essere mantenuti soltanto se queste interrelazioni e dipendenze **funzionano correttamente**



# Interdipendenze dell'infrastruttura



# Interdipendenze dell'infrastruttura


- Gli incidenti all'interno di un'infrastruttura critica possono avere **conseguenze di vasta portata** su molte altre infrastrutture. così come la **società nel suo complesso**
  - 2021 Hacking del gasdotto coloniale negli USA
  - 2019 Interruzioni di corrente in Venezuela e Argentina
  - 2017 Ripartizione logistica internazionale Moeller-Maersk

## US petrol supplies tighten after Colonial Pipeline hack Venezuela blackout: what caused it and what happens next? New malware hits JNPT operations as APM Terminals hacked globally

AP Moller-Maersk, one of the affected entities globally, operates the Gateway Terminals India (GTI) at JNPT, which has a capacity to handle 1.8 million standard container units

92 SHARES

By: PTI | Mumbai | Updated: June 27, 2017 11:09:54 pm



The official explained that JNPT is trying to help the company, but there is little that others can do as the problem is with the systems.

Operations at one of the three terminals of the nation's largest container port JNPT were impacted Tuesday as a fallout of the global ransomware attack, which crippled some central banks and many large corporations in Europe. AP Moller-Maersk, one of the affected entities globally, operates the Gateway Terminals India (GTI) at JNPT, which has a capacity to handle 1.8 million standard container units.

"We have been informed that the operations at GTI have come to a standstill because their systems are down (due to the malware

DER NEUE PEUGEOT 308

JUST ADD FUEL

4 JAHRE VOLLEKASKO  
4 JAHRE GARANTIE  
4 JAHRE WARTUNG  
4 WINTERRÄDER

IM ABO AB € 308,- MTL. 17€  
PLUS 3 MONATSRATEN GESCHENKT

TOP NEWS

CHSE Odisha +2 12th Result 2018 LIVE  
Updates: Pass percentage drops in Arts, increases in Science

Mumbai rains LIVE  
Updates: Monsoon hits Mumbai, two flights diverted, trains running late

India vs Pakistan: India beat Pakistan by 7 wickets to reach Women's Asia Cup final

• LIVE BLOG

Narendra Modi in China LIVE updates: Ni hao Qingdao! PM receives warm welcome on arrival

CyberSecPro

CC BY NC SA

# Interdipendenze dell'infrastruttura

- Gli incidenti all'interno di un'infrastruttura critica possono avere **conseguenze di vasta portata** su molte altre infrastrutture. così come la **società nel suo complesso**
  - 2021 Hacking del gasdotto coloniale negli USA
  - 2019 Interruzioni di corrente in Venezuela e Argentina
  - 2017 Ripartizione logistica internazionale Moeller-Maersk


## US petrol supplies tighten after Colonial Pipeline hack Venezuela blackout: what caused it and what happens next? New malware hits JNPT operations as APM Terminals hacked globally

AP Moller-Maersk, one of the affected entities globally, operates the Gateway Terminals India (GTI) at JNPT, which has a capacity to handle 1.8 million standard container units

92 SHARES

SHARE

By: PTI | Mumbai | Updated: June 27, 2017 11:09:54 pm



The official explained that JNPT is trying to help the company, but there is little that others can do as the problem is with the systems.

Operations at one of the three terminals of the nation's largest container port JNPT were impacted Tuesday as a fallout of the global ransomware attack, which crippled some central banks and many large corporations in Europe. AP Moller-Maersk, one of the affected entities globally, operates the Gateway Terminals India (GTI) at JNPT, which has a capacity to handle 1.8 million standard container units.

"We have been informed that the operations at GTI have come to a standstill because their systems are down (due to the malware

DER NEUE PEUGEOT 308

JUST ADD FUEL

4 JAHRE VOLLEKASKO  
4 JAHRE GARANTIE  
4 JAHRE WARTUNG  
4 WINTERRÄDER

0€\* ANFANGSLEISTUNG

IM ABO AB € 308,- MTL. 17€ PLUS 3 MONATSRATEN GESCHENK

TOP NEWS

CHSE Odisha +2 12th Result 2018 LIVE  
Updates: Pass percentage drops in Arts, increases in Science

Mumbai rains LIVE  
Updates: Monsoon hits Mumbai, two flights diverted, trains running late

India vs Pakistan: India beat Pakistan by 7 wickets to reach Women's Asia Cup final

Partnership By TRAVELSMART

• LIVE BLOG

Narendra Modi in China LIVE updates: Ni hao Qingdao! PM receives warm welcome on arrival

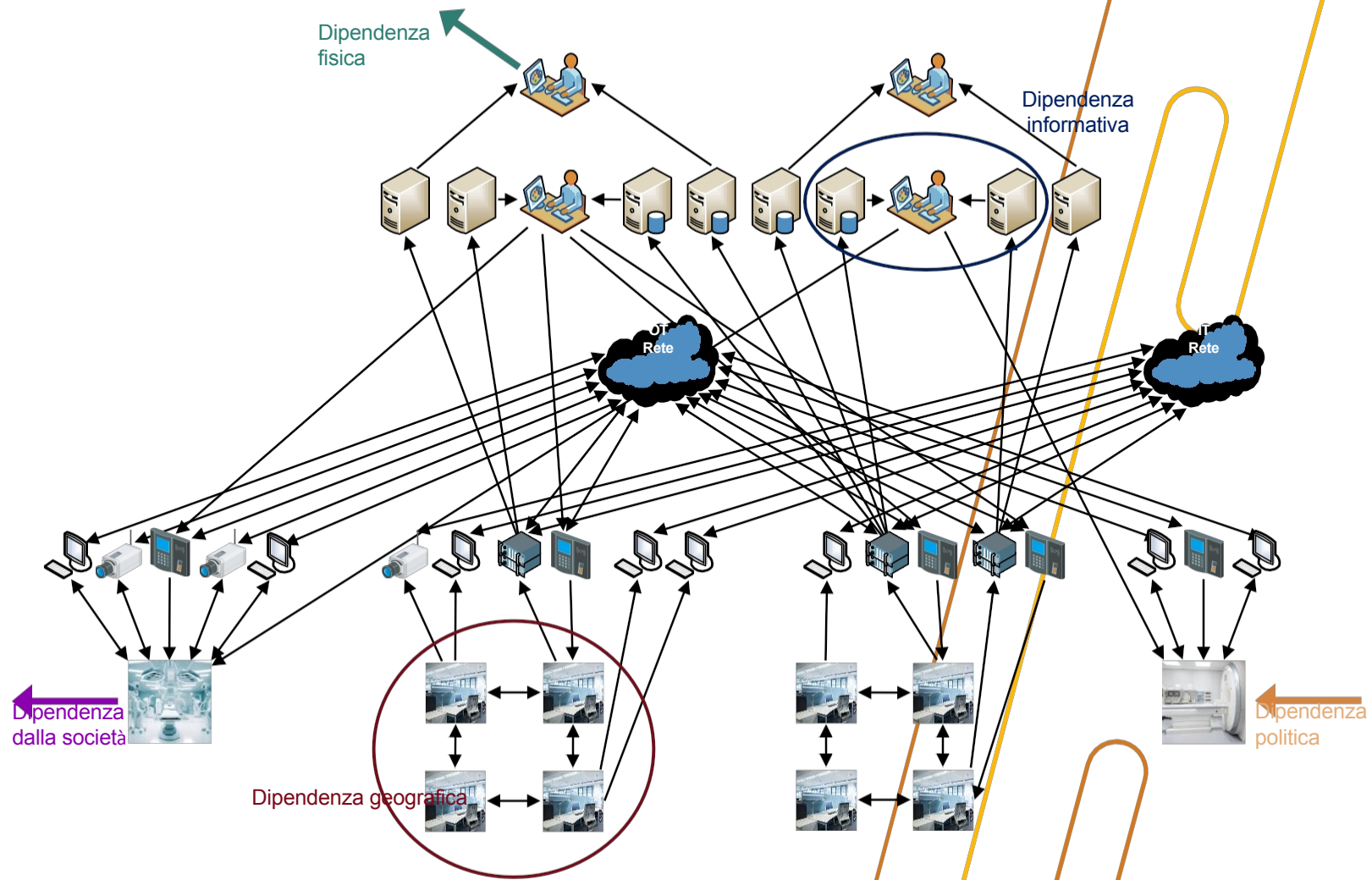
# Interdipendenza Tipi

- Le dipendenze devono essere **identificate e valutate** per un'analisi dei rischi.
- Analisi completa delle **dipendenze di un'infrastruttura critica**
  - Considerando sia le connessioni in entrata che quelle in uscita
  - Considerare le dipendenze negli impatti potenziali
  - Considerare le dipendenze dalle minacce potenziali
- Gli effetti a cascata possono verificarsi a causa delle dipendenze.
  - L'impatto di una minaccia si ripercuote sul **funzionamento di altre infrastrutture critiche**.
  - Il deterioramento può **influire** anche **su altre infrastrutture**.
  - Cause apparentemente insignificanti hanno un grande effetto
  - **Gli effetti a cascata** spesso non vengono considerati nel dettaglio

# Interdipendenza Tipi

- Nella letteratura iniziale si possono trovare diversi **tipi di dipendenze**
  - Dipendenza fisica
  - Dipendenza dalle informazioni
  - Dipendenza geografica
  - Dipendenza politica/procedurale
  - Dipendenza sociale/sociale
- Il tipo di dipendenza determina l'**influenza di una minaccia specifica**.
  - Per alcuni tipi, un incidente viene percepito **immediatamente** e anche in **modo più forte**.
  - In altri , le influenze **non si verificano direttamente** o hanno solo un impatto minore.
  - Alcuni effetti si diffondono solo quando è presente un **certo tipo di dipendenza**

# Interdipendenze dell'infrastruttura



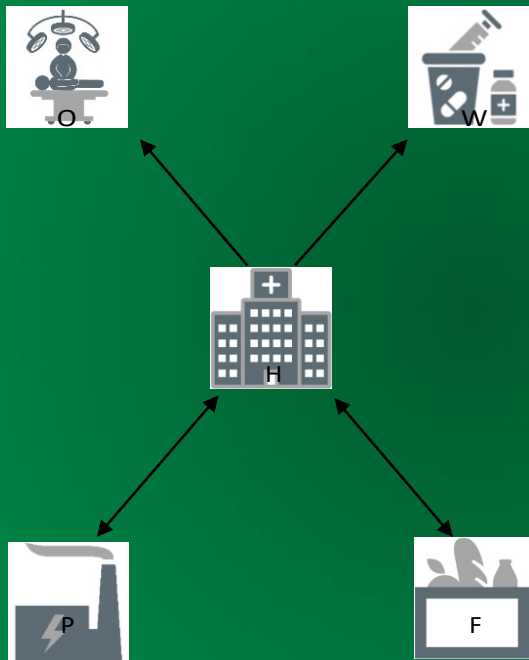
# Interpretazioni inedite

- Negli approcci reali, **non tutti i tipi di dipendenza sono rilevanti**.
  - L'utilizzo di tutti i tipi rende la descrizione del sistema complessivo **molto complessa**.
  - In particolare, le dipendenze politiche e sociali possono essere **molto vaghe**.
  - Importanza e **grado di dipendenza** non facili da stimare
  - Ciononostante, sono interessanti quando si considerano le infrastrutture critiche.
- 
- **La dipendenza fisica e quella dalle informazioni (cyber)** sono più importanti nella vita aziendale di tutti i giorni
- 
- **La dipendenza geografica** è spesso rilevante nel contesto di disastri naturali o guasti tecnici

# Interpretazioni inedite

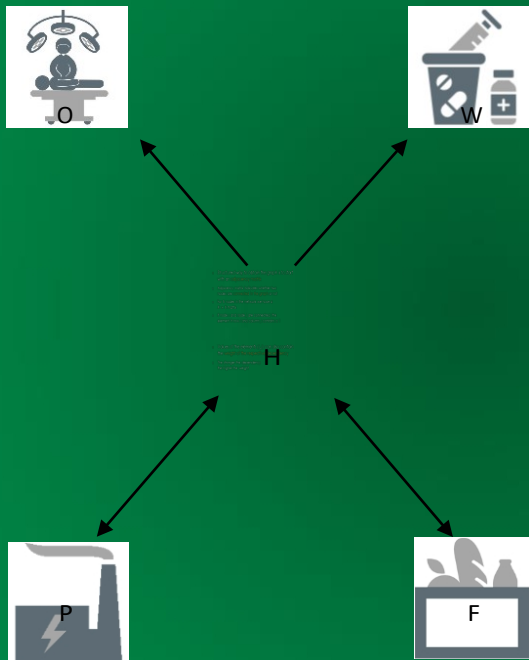
- La crescente **digitalizzazione** ha favorito una stretta relazione tra dipendenza fisica e cibernetica.
- I **sistemi cyber-fisici** sono al centro della maggior parte delle infrastrutture critiche
- Applicazione dei **sistemi di controllo industriale (ICS)** e dei sistemi di **controllo di supervisione e acquisizione dati (SCADA)**
- I processi fondamentali delle infrastrutture si basano su tali sistemi.
  
- Le infrastrutture critiche si sono evolute in **ecosistemi complessi e altamente sensibili** di sistemi cyber-fisici fortemente interconnessi.
  
- È importante considerare queste **interrelazioni sensibili** e le necessità di analisi e gestione del rischio delle infrastrutture critiche.

# Interdipendenza Grafici



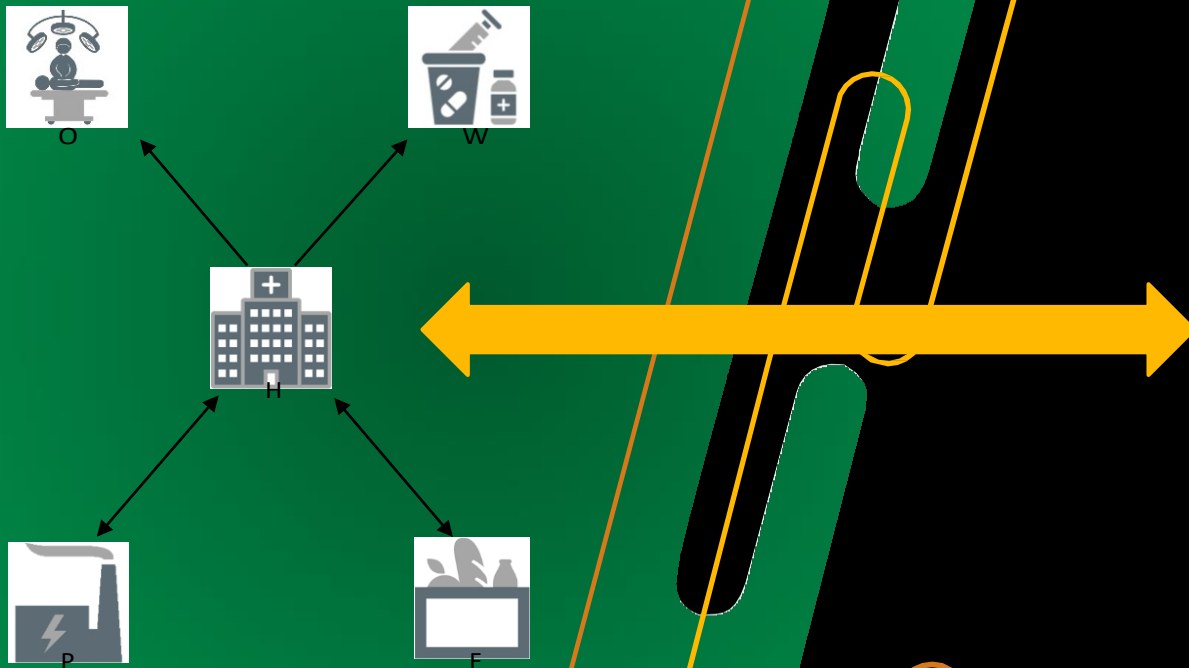
- È necessaria una forma più astratta per descrivere le dipendenze tra le infrastrutture critiche.
- Si può ottenere con un **grafico delle interdipendenze**
- I **nodi** rappresentano le infrastrutture critiche
- I **bordi** rappresentano le dipendenze tra loro
- I **bordi sono diretti**  
Cioè "P→ W" significa "W dipende da P".
- Il tipo specifico di dipendenza può essere trascurato
- Il grafico potrebbe contenere **bordi diversi** per la dipendenza fisica e cibernetica.
- Il grafico diventerebbe molto più complesso

# Interdipendenza Grafici



- Il modo strutturato per ottenere il grafo è quello di iniziare con una **matrice di adiacenza**
- La matrice di adiacenza indica se due nodi sono **collegati** o meno **nel grafo**.
- Per  $N$  nodi della rete abbiamo un  $N \times N$  matrice
- Se il nodo  $i$  e il nodo  $j$  sono collegati, l'elemento nella riga  $i$  e nella colonna  $j$  contiene un 1
- I valori degli elementi  $(i, j)$  possono contenere anche il **peso della rispettiva dipendenza**
- Più forte è la dipendenza, più alto è il peso

# Interdipendenza Grafici

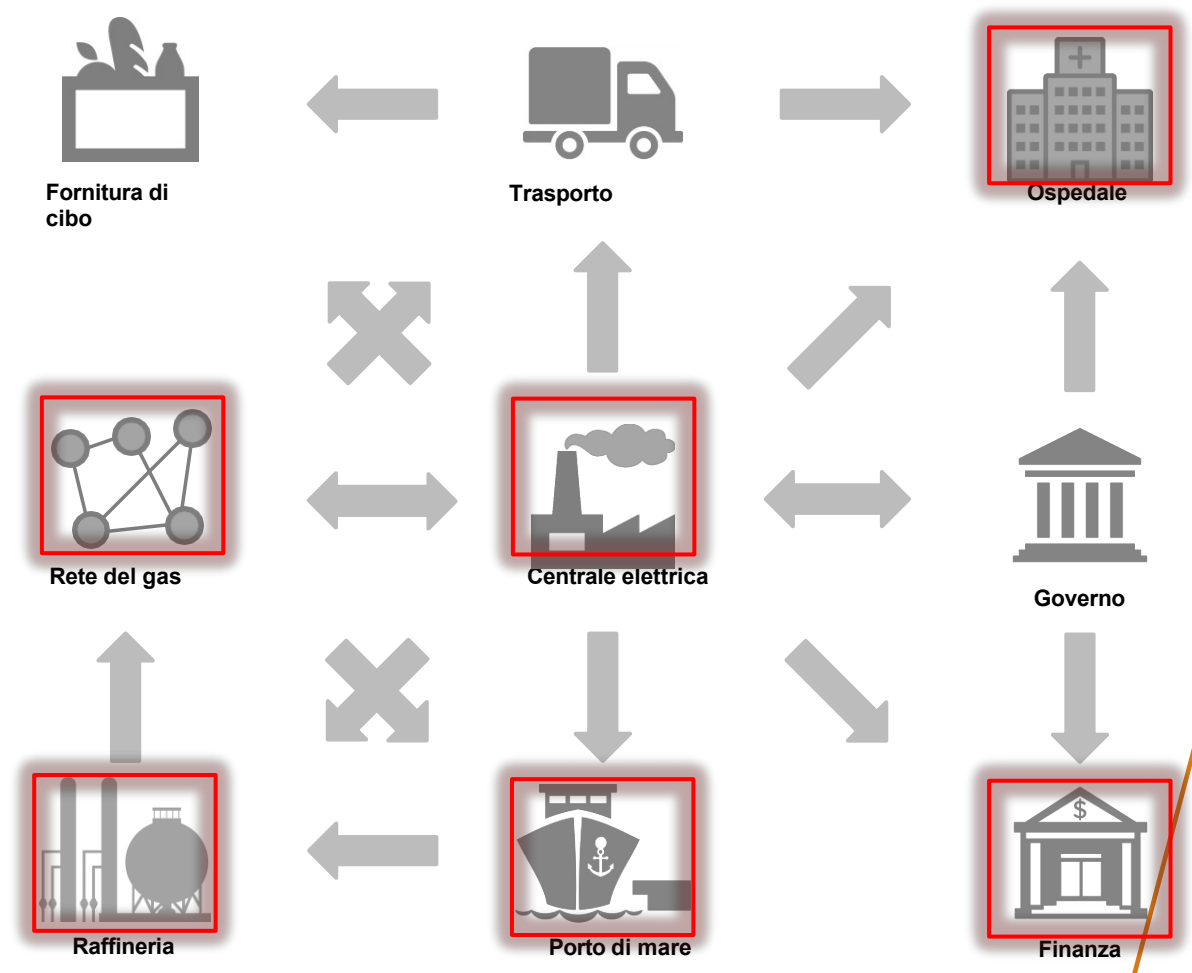


	P	T	W	H	F
P	0	0	1	0	0
T	0	0	1	0	0
W	0	0	0	1	1
H	0	0	0	0	0
F	0	0	0	0	0

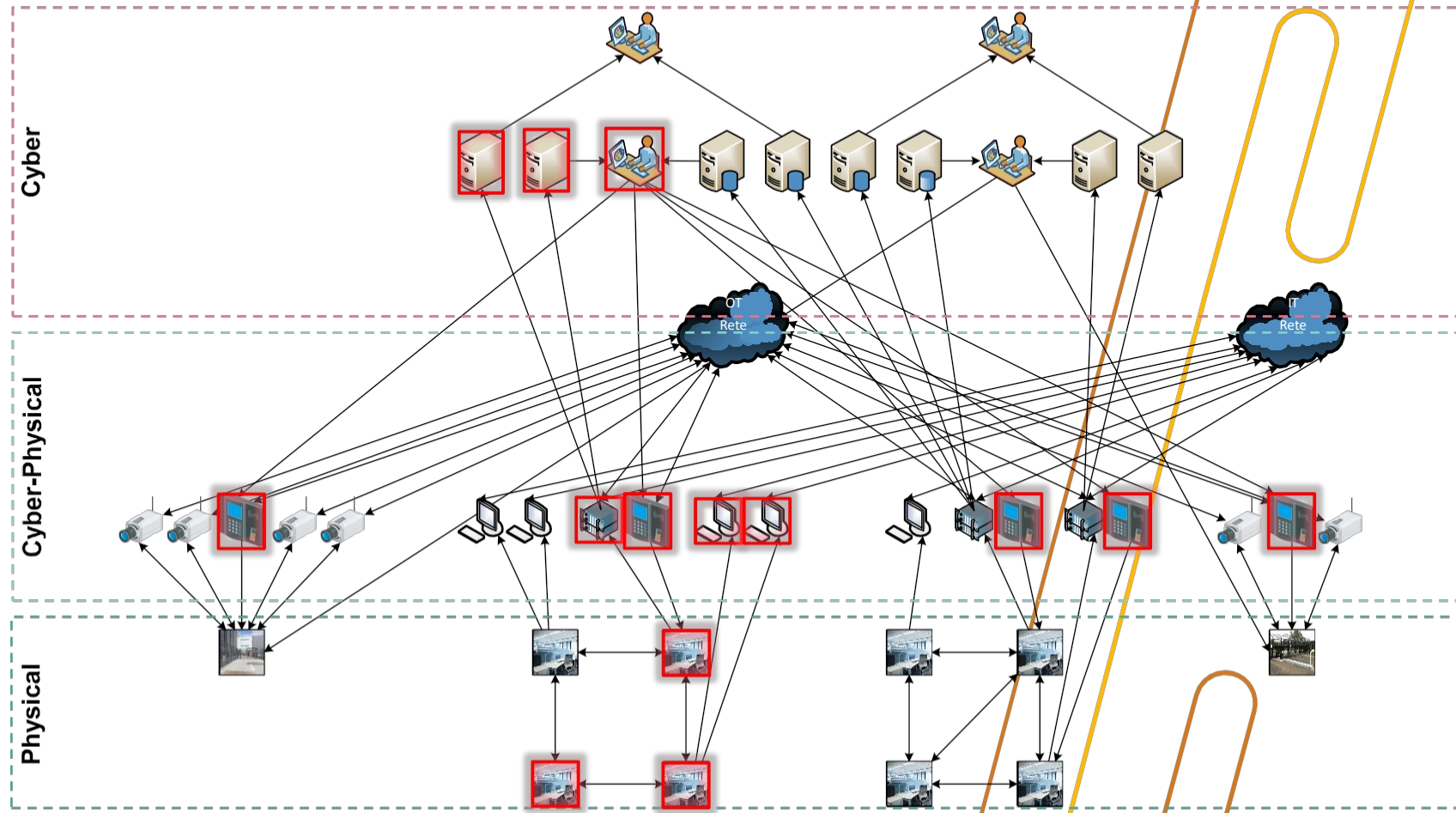
# Effetti a cascata

Come possono essere gli effetti a cascata modellato e analizzato?

# Effetti a cascata tra le infrastrutture



# Effetti a cascata tra le attività



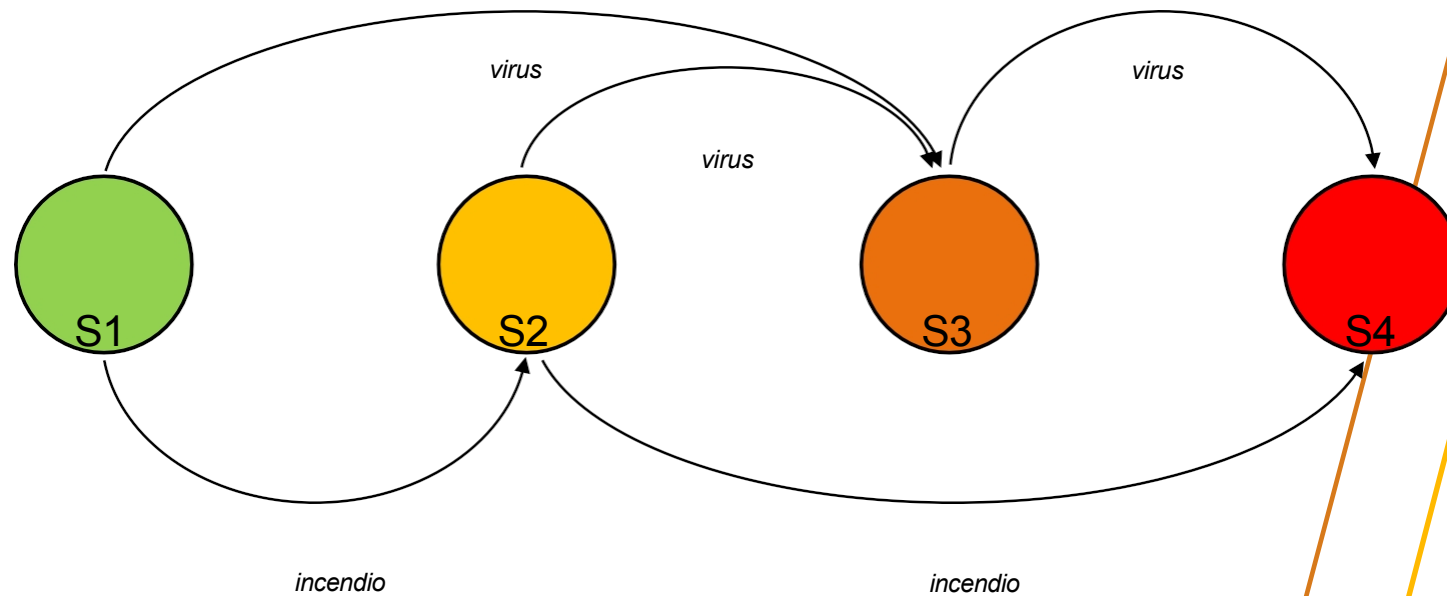
# Modellazione degli effetti a cascata

- Per descrivere lo stato di un'infrastruttura critica, un sistema binario **potrebbe non essere sufficiente**.
- "pienamente operativo" vs. "guasto completo".
- Nella vita reale, le infrastrutture possono avere **diversi stati operativi**.
- A seconda delle risorse disponibili, della capacità produttiva, ecc.
- Gli stati operativi possono **influenzare le infrastrutture dipendenti** in vari modi
- **Una scala più differenziata** per descrivere lo stato operativo di un'infrastruttura critica fornirà **una migliore comprensione** dell'evoluzione del sistema complessivo.

# Modellazione degli effetti a cascata

- Un approccio consiste nel modellare l'infrastruttura critica come un **automa o una macchina a stati**.
- Numero di **stati operativi diversi**
- **Rappresentazione astratta** dei vari stati in cui può trovarsi l'infrastruttura
- La descrizione dettagliata può essere formulata separatamente (ad esempio, specifiche interne, ecc.).
- **Transizioni ben definite tra questi stati**
- Conversione da uno stato all'altro
- La modifica dello stato si basa su un input specifico

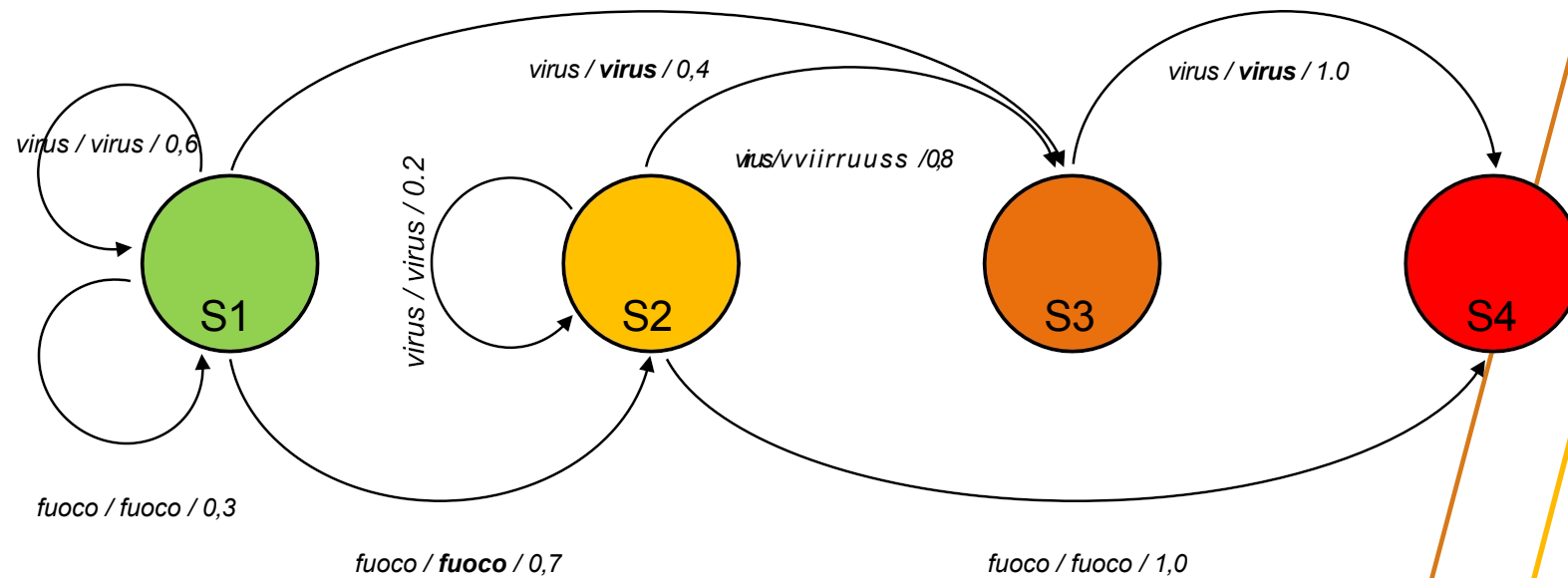
# Modellazione degli effetti a cascata



# Modellazione degli effetti a cascata

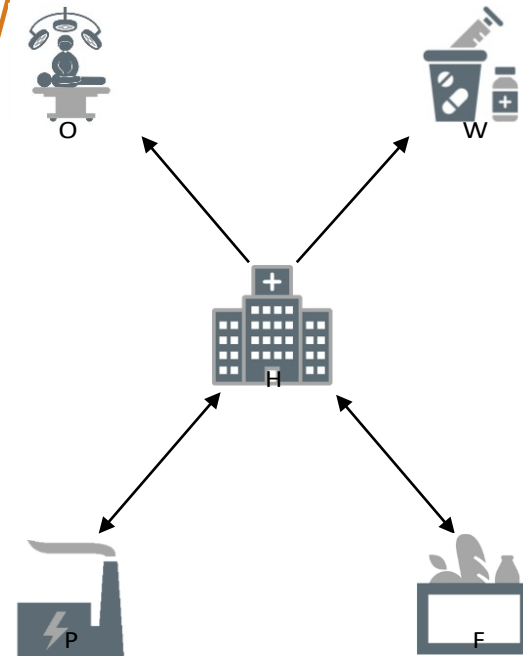
- Sono necessarie ulteriori informazioni per descrivere gli scenari reali.
- Gli Stati devono gestire **gli eventi di input** e fornire anche **eventi di output**.
  - L'incidente scatenante può avere origine da un'altra parte (ad esempio, un evento esterno).
  - Il cambiamento di stato può **innescare un altro evento** (ad esempio, un altro sistema interno).
- Le infrastrutture reagiranno in modo diverso in caso di eventi diversi.
  - **Lo stato attuale e l'evento scatenante** definiscono lo stato risultante
- Le transizioni non saranno **deterministiche**
  - Il funzionamento delle infrastrutture nella vita reale contiene troppe **incertezze**
  - **La probabilità** deve essere inclusa nelle transizioni.

# Modellazione degli effetti a cascata

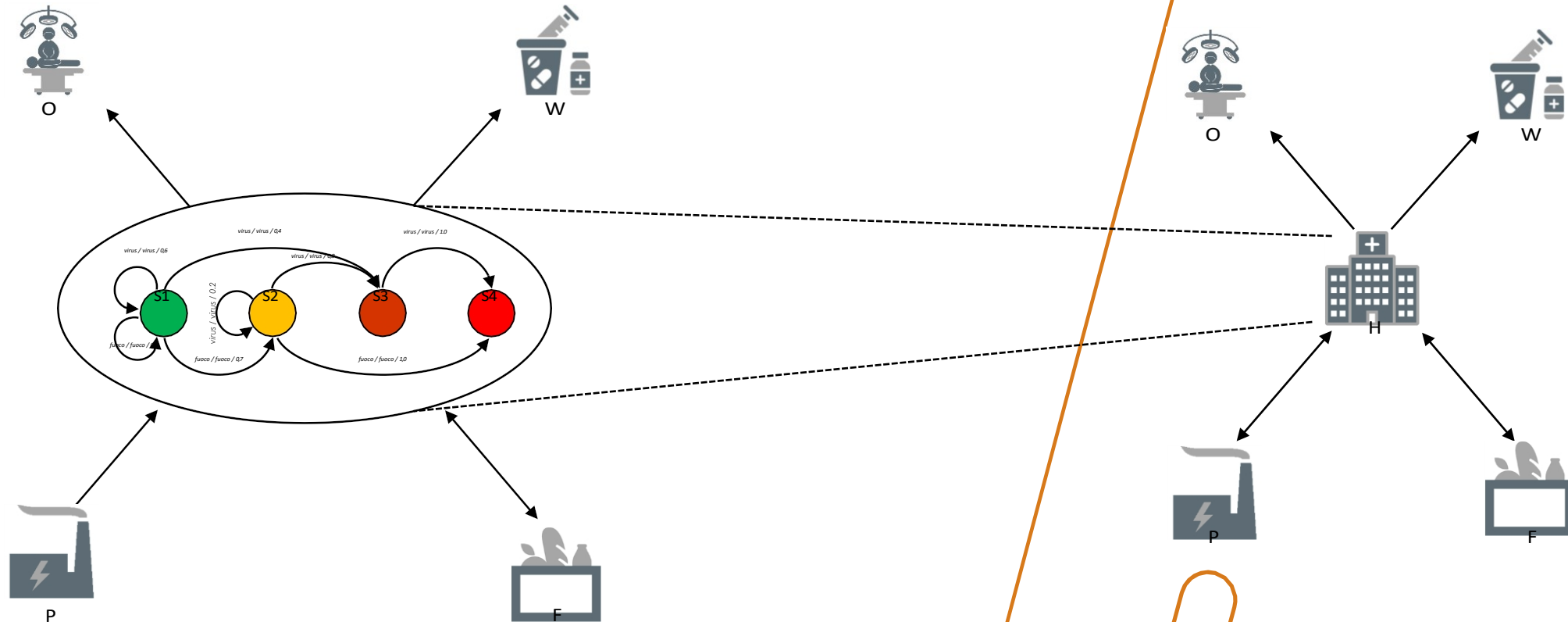


# Modellare gli effetti a cascata

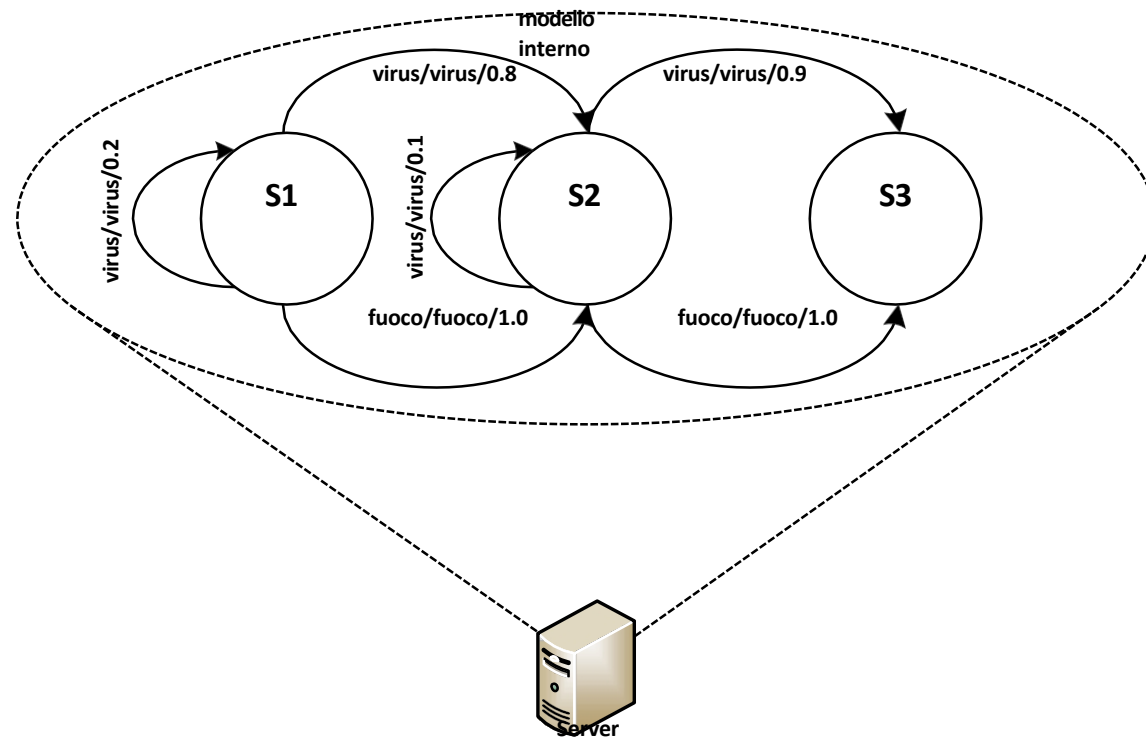
- Combinare questo approccio più dinamico con il **grafico delle interdipendenze**
- Ogni infrastruttura può trovarsi in **una delle seguenti posizioni diversi stati operativi**
  - Da "**pienamente operativo**" ("1") a "**guasto completo**" ("3")
- La modifica dello stato operativo si basa su
  - le **infrastrutture dei fornitori**
  - un **evento esterno** (ad esempio, un incidente)
- Il cambiamento dello stato operativo avviene con una **specifica probabilità**



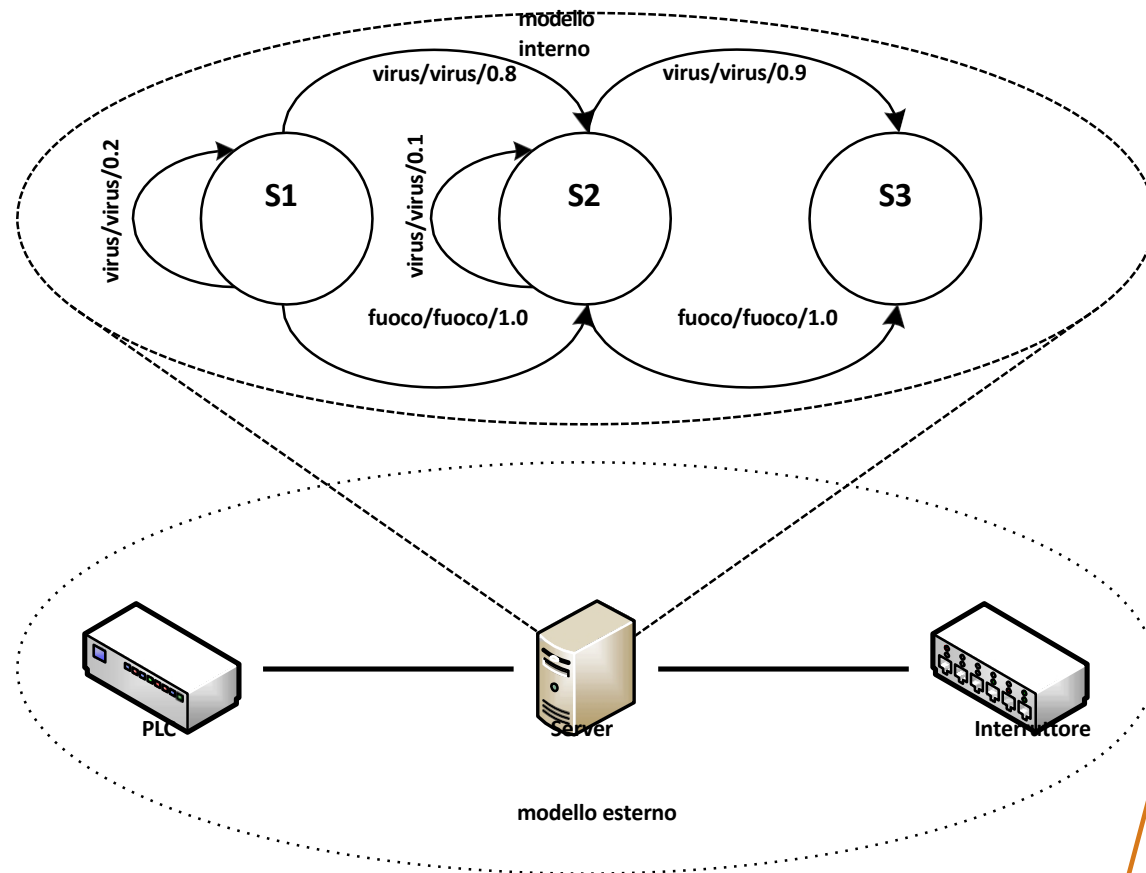
# Modellare gli effetti a cascata



# Modellare gli effetti a cascata



# Modellare gli effetti a cascata



# Simulazione degli effetti a cascata

- Il modello di simulazione descrive l'**evoluzione dell'intera rete di infrastrutture critiche**.
  - Il modello di rischio stocastico viene istanziato
  - Viene eseguito **un gran numero di simulazioni** per valutare un incidente specifico che si verifica su un'infrastruttura
- L'incidente/attacco modifica lo **stato operativo dell'IC di destinazione**.
  - Anche gli IC dipendenti cambiano il loro stato (secondo la distribuzione di probabilità)
  - Gli effetti dell'incidente **si propagano attraverso la rete di infrastrutture critiche**.
- L'impatto totale è misurato sulla base dello **stato finale di tutti gli IC** al termine della simulazione

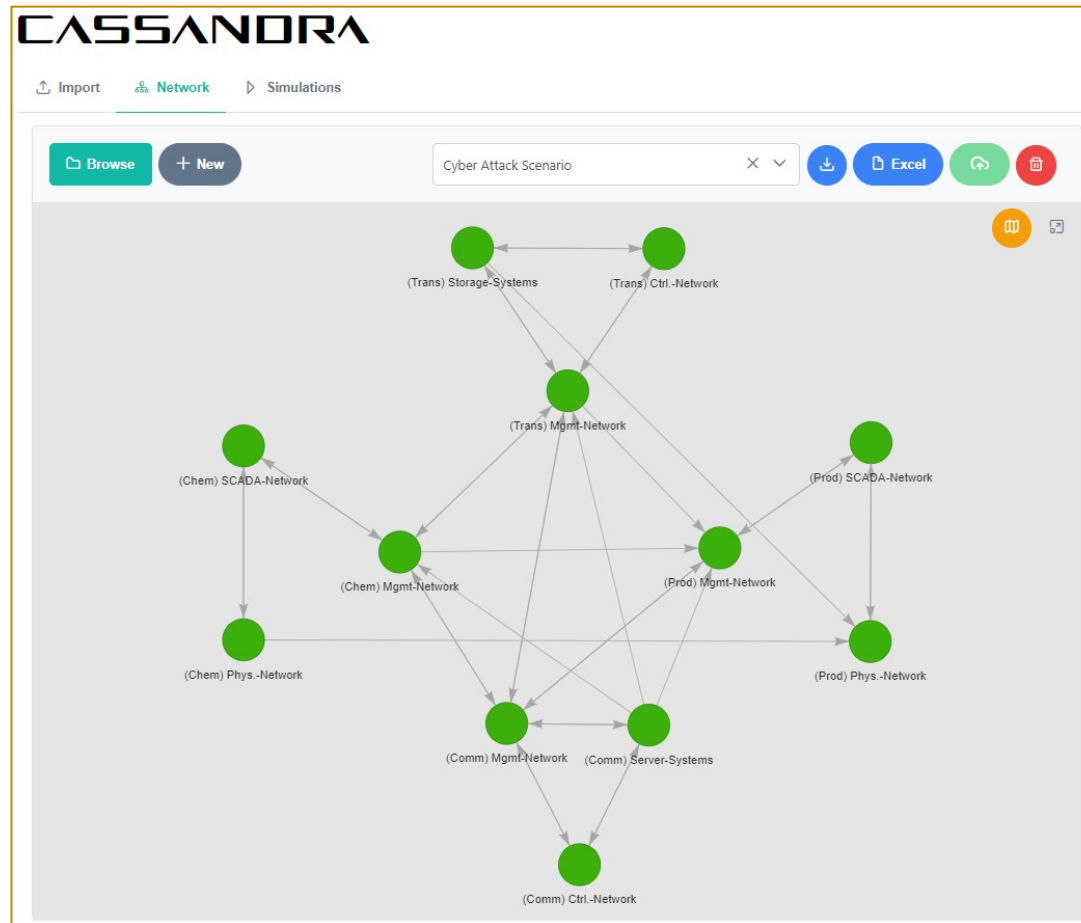
# Simulazione degli effetti a cascata

- Il modello di simulazione è stato implementato nel progetto SAURON.
- L'attenzione si concentra **sulle risorse fisiche e informatiche** dei porti marittimi.
  - Modellare vari asset nel dominio fisico e cibernetico.
  - Definire gli **stati operativi**
  - Specificare le **interdipendenze** tra loro
  - Definire **le probabilità di transizione**
- È possibile simulare scenari con **incidenti provenienti da domini diversi**.
  - Incidente fisico che colpisce il dominio cibernetico
  - Incidente informatico che colpisce il mondo fisico

# Simulazione degli effetti a cascata

- Lo strumento registra tutti i **cambiamenti di stato** e gli **stati finali** di ciascuna esecuzione di simulazione
- I cicli di simulazione restituiscono una **panoramica sull'evoluzione del sistema**
  - Quale asset è stato "infettato" in quale passaggio
  - Qual è il nuovo stato dell'asset
  - Quale asset ha causato il cambiamento di stato
- Gli stati finali riflettono l'**impatto complessivo di un incidente** sull'infrastruttura.
- È possibile generare diverse visualizzazioni e report
  - **Stato finale medio** di un bene
  - **Scenario medio**
  - **Lo scenario peggiore**

# Simulazione degli effetti a cascata



# Simulazione degli effetti a cascata

**CASSANDRA** Impressum API

Import Network **Simulations**

Alert Source: (Chem) Mgmt-Network

Trigger: Cyber\_Attack

Number of simulations: 100

Run Simulation

Simulations Analysis Simulation Cases Simulation Statistics

Simulation 1  
Average node state: 4.06

Time	Entity Name	Event	New State	Because Of
0	(Chem) Mgmt-Network	Cyber_Attack	4	
1	(Trans) Mgmt-Network	mgmt_system_infiltrated	4	(Chem) Mgmt-Network
1	(Prod) Mgmt-Network	mgmt_system_infiltrated	4	(Chem) Mgmt-Network
1	(Chem) SCADA-Network	mgmt_system_infiltrated	4	(Chem) Mgmt-Network
2	(Trans) Ctrl.-Network	mgmt_system_infiltrated	4	(Trans) Mgmt-Network
2	(Comm) Mgmt-Network	mgmt_system_infiltrated	4	(Trans) Mgmt-Network
2	(Prod) SCADA-Network	mgmt_system_infiltrated	3	(Prod) Mgmt-Network
2	(Chem) Phys.-Network	scada_system_infiltrated	5	(Chem) SCADA-Network
3	(Trans) Storage-Systems	scada_system_infiltrated	5	(Trans) Ctrl.-Network
3	(Comm) Ctrl.-Network	mgmt_system_infiltrated	4	(Comm) Mgmt-Network
3	(Prod) Phys.-Network	scada_system_alerted	3	(Prod) SCADA-Network
4	(Comm) Server-Systems	ctrl_system_infiltrated	5	(Comm) Ctrl.-Network

# Connettersi con CyberSecPro: come registrarsi e altre informazioni pratiche

1. Sito web:  
[www.cybersecpro-project.eu](http://www.cybersecpro-project.eu)
2. X (Twitter):  
[https://twitter.com/CyberSecPro\\_eu](https://twitter.com/CyberSecPro_eu)
3. LinkedIn: <https://www.linkedin.com/company/cybersecpro-euproject/>



**Co-funded by  
the European Union**

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

 ACEEU ACCREDITATION COUNCIL FOR ENTREPRENEURIAL & ENGAGED UNIVERSITIES	 AIT AUSTRIAN INSTITUTE OF TECHNOLOGY	 APIROPLUS SOLUTIONS	 SINTEF	 SOCIAL ENGINEERING ACADEMY	 TAL TECH
ACEEU GmbH Germany <a href="#">Visit Website</a>	AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH Austria <a href="#">Visit Website</a>	APIROPLUS SOLUTIONS LTD Cyprus <a href="#">Visit Website</a>	SINTEF AS Norway <a href="#">Visit Website</a>	Social Engineering Academy GmbH Germany <a href="#">Visit Website</a>	Tallin University of Technology Estonia <a href="#">Visit Website</a>
Logo missing	 COFAC COOPERATIVA DE FORMAÇÃO E ANIMACÃO CULTURAL C.R.L.	 Consiglio Nazionale delle Ricerche	 Technische Universität Braunschweig	 TECHNICAL UNIVERSITY OF CRETE	 trustilio Enhance your Trustworthiness
C2B CONSULTING <a href="#">Visit Website</a>	COFAC Portugal <a href="#">Visit Website</a>	Consiglio Nazionale delle Ricerche Italy <a href="#">Visit Website</a>	Technical University of Braunschweig Germany <a href="#">Visit Website</a>	Technical University of Crete Greece <a href="#">Visit Website</a>	trustilio B.V. The Netherlands <a href="#">Visit Website</a>
 focal point Cyber Defence Exercises as a Service	 GOETHE UNIVERSITÄT FRANKFURT AM MAIN	 ITML	 UNINOVA	 UNIVERSIDAD DE MÁLAGA	 NOVA UNIVERSIDADE NOVA DE LISBOA
FDICAL POINT Belgium <a href="#">Visit Website</a>	Goethe University Frankfurt Germany <a href="#">Visit Website</a>	Information Technology for Market Leadership Greece <a href="#">Visit Website</a>	Uninova Portugal <a href="#">Visit Website</a>	Universidad de Malaga Spain <a href="#">Visit Website</a>	Universidade Nova De Lisboa Portugal <a href="#">Visit Website</a>
 Institut Mines-Télécom	 LAUREA	 GRUPPO Maggioli	 University of Cyprus	 FACULTY OF SCIENCES NOVI SAD SERBIA	 UNIVERSITY OF PIRAEUS RESEARCH CENTER
Institut Mines-Télécom France <a href="#">Visit Website</a>	Laurea University of Applied Sciences Finland <a href="#">Visit Website</a>	Maggioli S.p.A. Italy <a href="#">Visit Website</a>	University of Cyprus Cyprus <a href="#">Visit Website</a>	University of Novi Sad Faculty of Sciences Serbia <a href="#">Visit Website</a>	University of Piraeus Research Center Greece <a href="#">Visit Website</a>
 PDMFC	 Security Labs Consulting Ltd	 SGI	 Zelus		
PDMFC Portugal <a href="#">Visit Website</a>	Security Labs Consulting Ltd Ireland (Republic) <a href="#">Visit Website</a>	Serious Games Interactive Denmark <a href="#">Visit Website</a>	ZELUS P.C. Greece <a href="#">Visit Website</a>		

# Grazie

Si prega di inviare tutte le domande a:  
Stefan Schauer, [Stefan.Schauer@ait.ac.at](mailto:Stefan.Schauer@ait.ac.at)  
Abdelkader Shaaban  
[abdelkader.Shaaban@ait.ac.at](mailto:abdelkader.Shaaban@ait.ac.at)