



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

Cascading Effects in Complex Maritime Networks and Supply Chains

CSP008_S_M

PRESENTATION BY:
DR. STEFAN SCHAUER
DR. ABDELKADER SHAABAN
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY





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

Acknowledgement

- *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*

Cascading Effects in Complex Maritime Networks and Supply Chains

Overview

- Topic-1: Introduction to Critical Infrastructure
- Topic-2: Threat Landscape in the Maritime Sector
- Topic-3: Critical Infrastructure Interdependence
- Topic-4: Cascading Effects and their Impacts
- Topic-5: Simulating and Analysing Cascading Effects

Agenda

- 1. Critical Entities
- 2. Interdependencies
- 3. Cascading Effects
- 4. Example: Cascading Effects

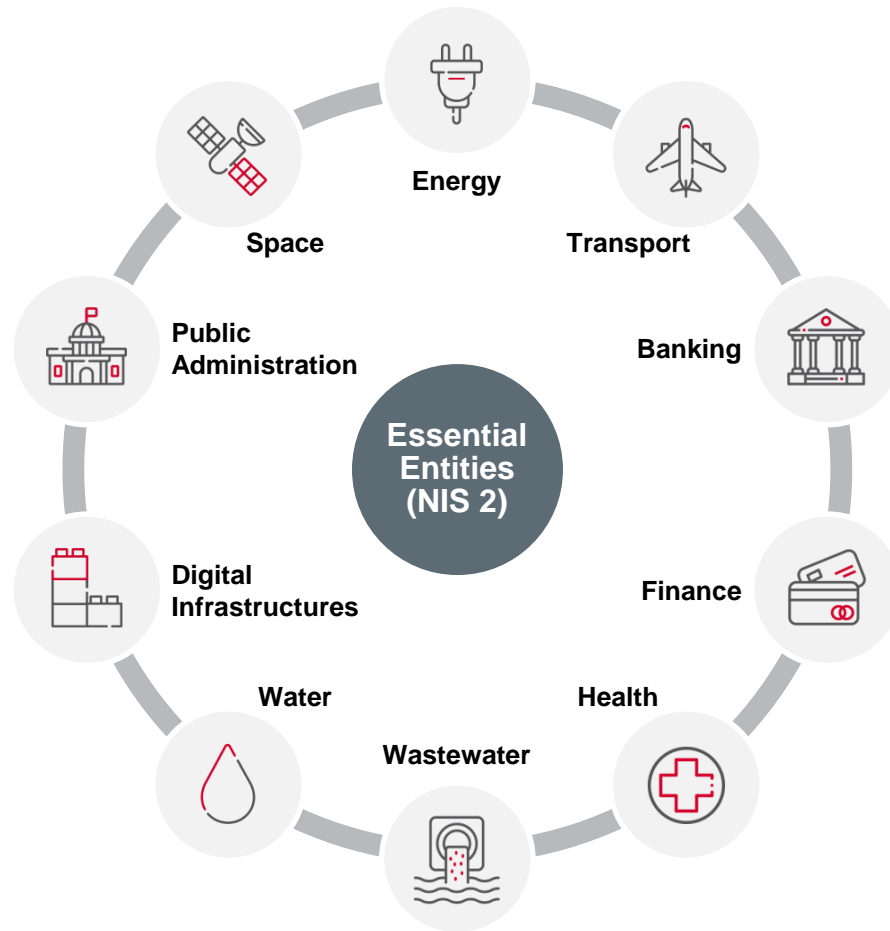
Critical Entities

What are critical infrastructures and the critical assets therein?

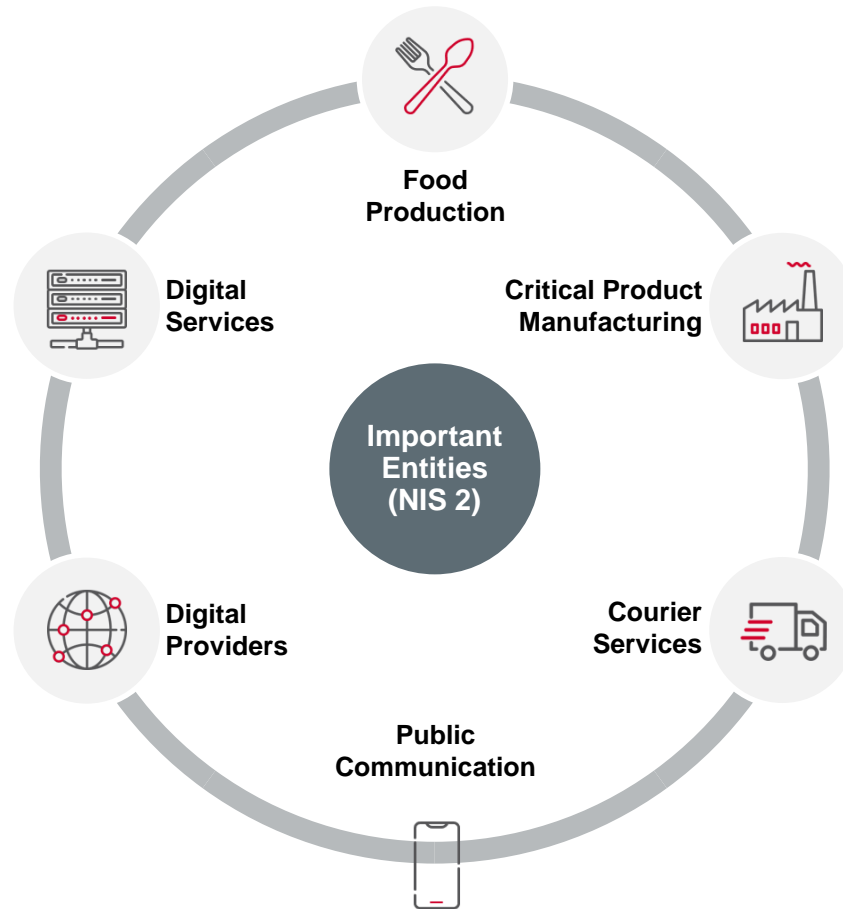
Critical Infrastructures

- Critical infrastructures (CIs) are essential for the **maintenance of vital societal functions**
- Basic **supply chain networks** (electricity, gas, water)
- Information and communication **(ICT) networks**
- Complex systems with **high social impact** (medical care, finance, transportation networks)

Critical Infrastructures



Critical Infrastructures



Critical Infrastructures



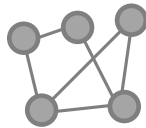
Food Supply



Transportation



Hospital



Gas Network



Power Plant



Government



Refinery



Sea Port

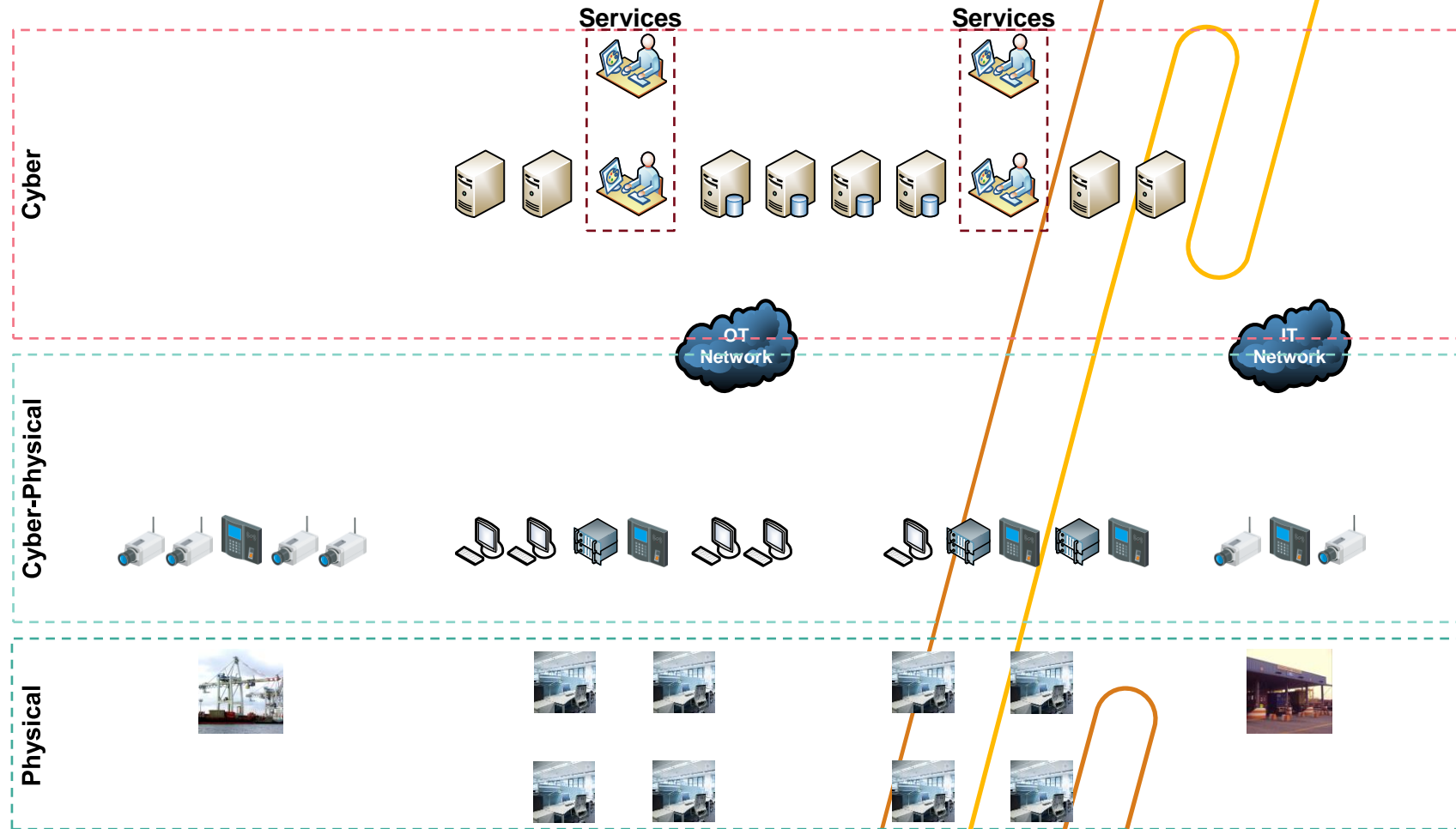


Finance

Critical Assets

- Within critical infrastructures or organisations in general
critical assets or components can be defined
 - Provide **core functionalities** for the organisation
 - Required for **maintaining the service** of the organisation
- Such critical assets or components can be located in **different domains**
 - **Physical**: essential parts of the utility network (pumps, substations, pipes, etc.)
 - **Cyber-Physical**: monitoring and control systems (PLCs, sensors, switches, etc.)
 - **Cyber**: virtual infrastructure and software (servers, databases, applications)

Critical Assets

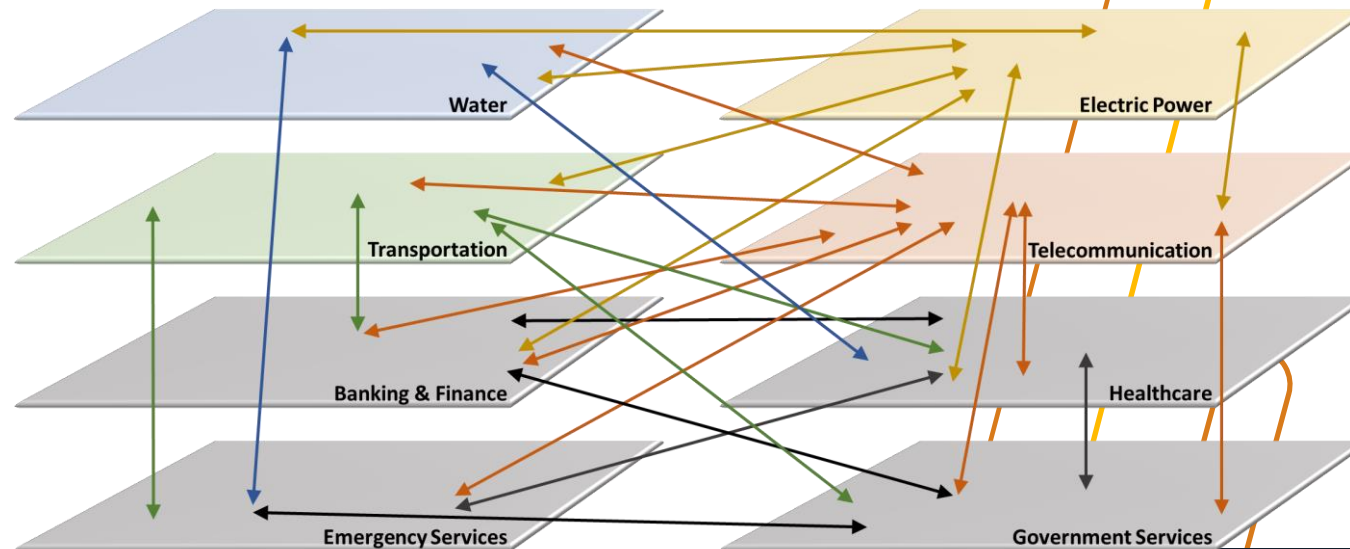


Interdependencies

How can dependencies among critical entities be characterised?

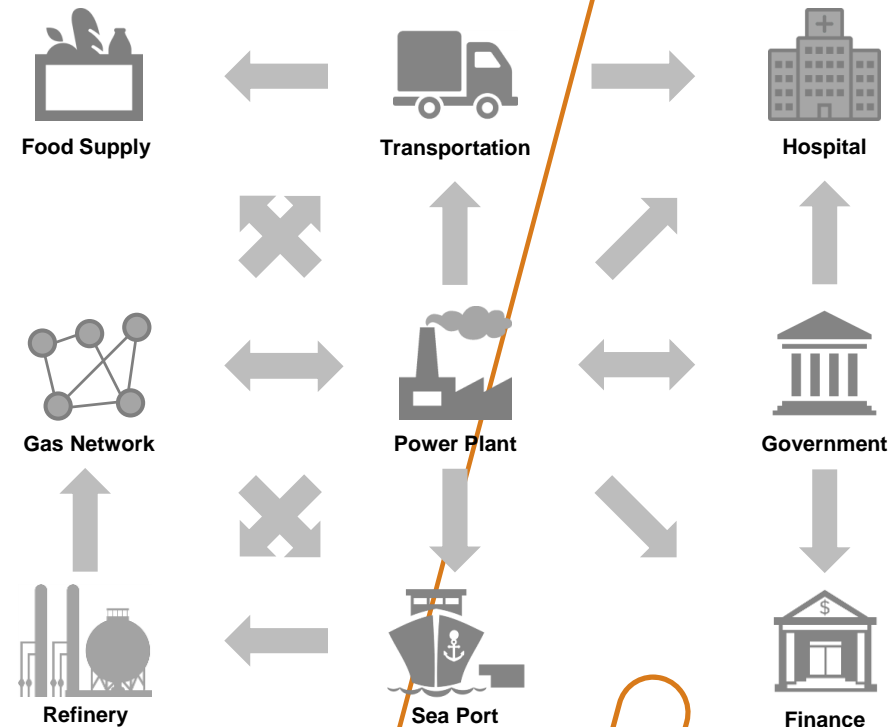
Infrastructure Interdependencies

- Over the last decades critical entities have become more and more **interrelated and interdependent**
 - Complex **service provider and consumer** relations among entities
 - Interwoven and often **fragile supply chains** on a national and international scale



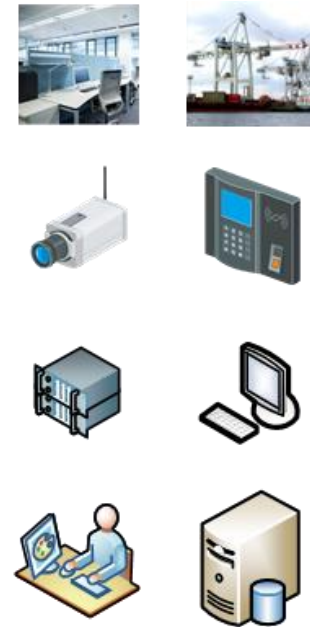
Infrastructure Interdependencies

- Critical infrastructures cannot be considered in isolation
- Infrastructures act as suppliers of **different resources and services**
- Infrastructures also act as **consumers** of certain **resources and services** of other infrastructures to ensure functionality

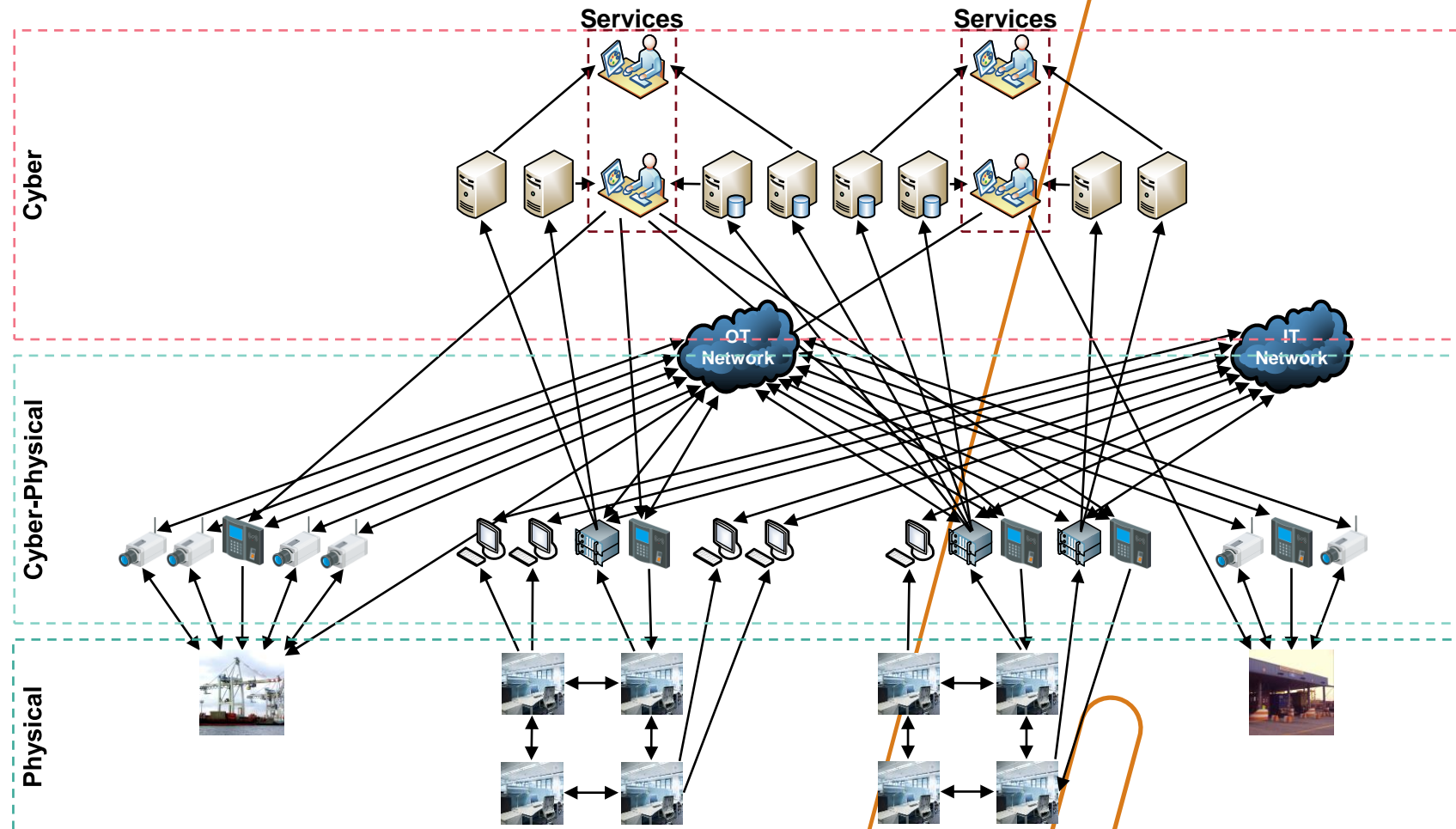


Infrastructure Interdependencies

- Interdependencies exist also **within organisations** and **among their premises** due to the **increase of digitalisation and data exchange**
 - **Buildings and machinery** are “smart” and are connected to digital systems
 - **Video surveillance and access control** systems can influence physical assets
 - **Sensors and Internet of Things (IoT)** devices connect physical and cyber assets
 - **Services** are provided by **applications** running on real or virtual servers
- Functionality and services of an infrastructure can only be maintained if these interrelations and dependencies are **working properly**



Infrastructure Interdependencies



Infrastructure Interdependencies

- Incidents within one critical infrastructure can have **far-reaching consequences** among multiple other infrastructures as well as **society as a whole**
 - 2021 Hacking of the Colonial Pipeline in USA
 - 2019 Power outages in Venezuela and Argentina
 - 2017 International Moeller-Maersk logistics breakdown

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

ADVERTISMENT

DER NEUE PEUGEOT 308

JUST ADD FUEL

4 JAHRE VOLLEKASKO
4 JAHRE GARANTIE
4 JAHRE WARTUNG
4 WINTERRÄDER

0€ ANSCHULUNG

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

ADVERTISMENT

TRAVEL SMART

Partnership By

WOLFPACK

LIVE BLOG

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

5 mins ago

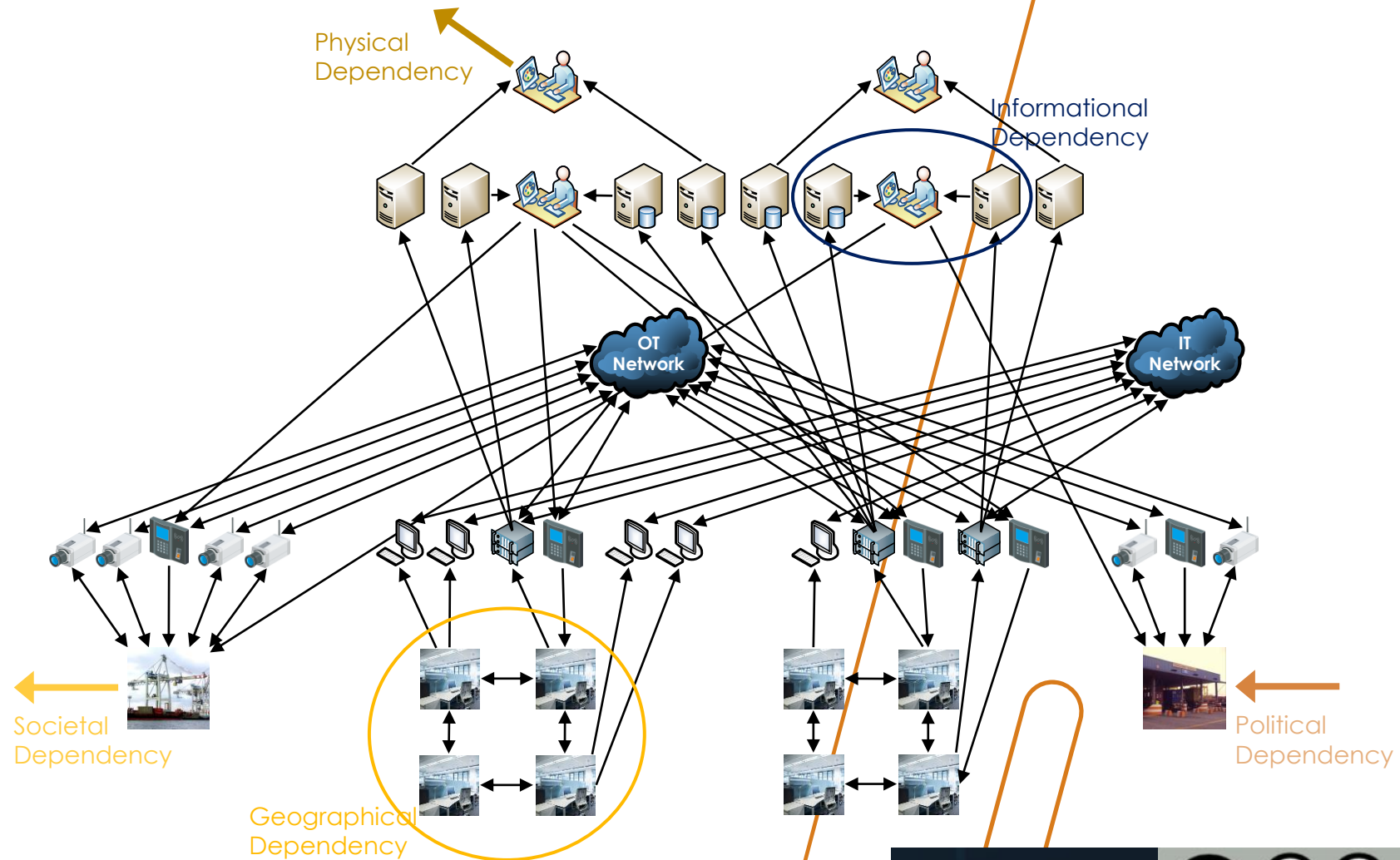
Interdependency Types

- Dependencies need to be **identified and evaluated** for a risk analysis
- Comprehensive analysis of the **dependencies of a critical infrastructure**
 - Considering both incoming and outgoing connections
 - Considering dependencies in potential impacts
 - Considering dependencies on potential threats
- Cascading effects can occur due to dependencies
 - Impact of a threat affects the **operation of other critical infrastructures**
 - Impairment can again have an **influence on other infrastructures**
 - Apparently insignificant causes have a great effect
 - **Cascading effects** are often not considered in detail

Interdependency Types

- In early literature, several **types of dependencies** can be found
 - Physical dependency
 - Information dependency
 - Geographical dependency
 - Political/procedural dependency
 - Social/societal dependency
- Type of a dependency determines the **influence of a specific threat**
 - For some types, an incident is perceived **immediately** and also **stronger**
 - In other cases, influences do **not occur directly** or have only minor impact
 - Some effects only spread when a **certain type of dependency** is present

Infrastructure Interdependencies



Novel Interpretations

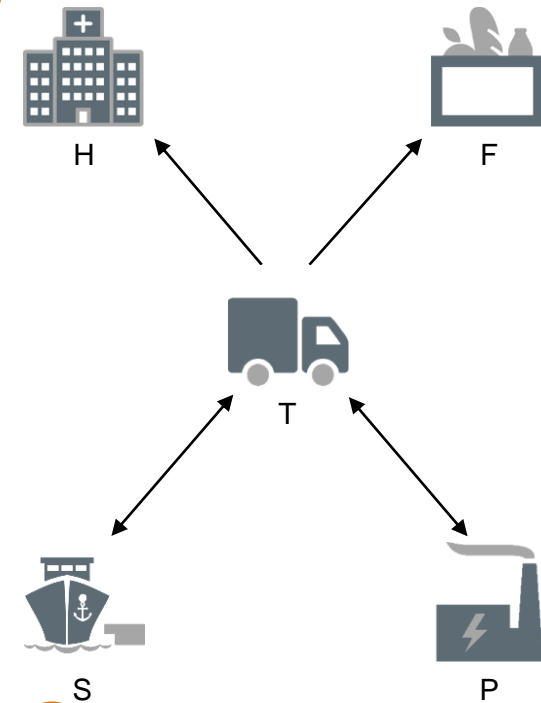
- In real-life approaches, **not all of those dependency types are relevant**
 - Using all types makes the description of the overall system **highly complex**
 - Particularly the political and societal dependencies can be **very vague**
 - Importance and **degree of dependency** not easy to estimate
 - Nevertheless they are of interest when looking at critical infrastructures
- **Physical and information (cyber) dependency** are more important in day-to-day business life
- **Geographical dependency** is often relevant in the context of natural disasters or technical failures

Novel Interpretations

- Increasing **digitalization** has fostered the tight relation between physical and cyber dependency
 - **Cyber-physical systems** are at the heart of most critical infrastructures
 - Application of **Industrial Control Systems** (ICS) and **Supervisory Control and Data Acquisition** (SCADA) systems
 - Infrastructures' core processes are building upon those systems
- Critical infrastructures have evolved into **complex and highly sensitive ecosystems** of strongly interconnected cyber-physical systems
- Important to consider these **sensitive interrelations** and needs to go into the risk analysis and risk management of critical infrastructures

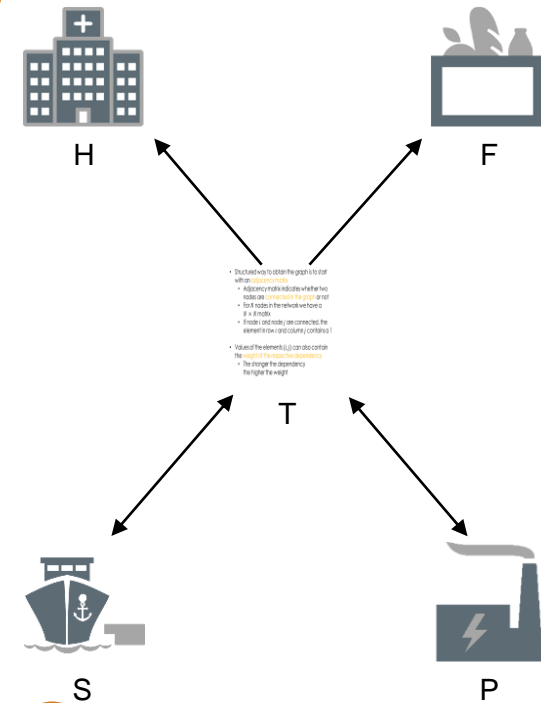
Interdependency Graphs

- More abstract form of describing the dependencies among critical infrastructures is required
- Can be achieved by an **interdependency graph**
 - **Nodes** represent critical infrastructures
 - **Edges** represent dependencies among them
 - **Edges** are directed
i.e. " $P \rightarrow W$ " means "W is depending on P"
- Specific type of the dependency can be neglected
 - Graph could contain **different edges** for physical and cyber dependency
 - Graph would become much more complex



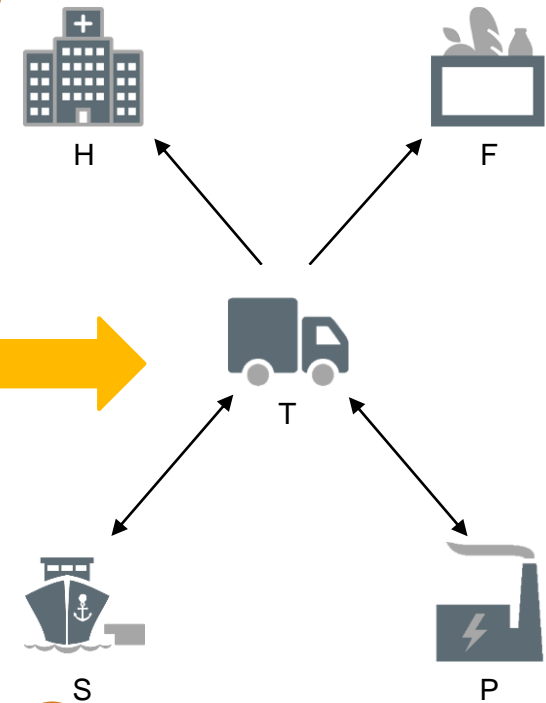
Interdependency Graphs

- Structured way to obtain the graph is to start with an **adjacency matrix**
 - Adjacency matrix indicates whether two nodes are **connected in the graph** or not
 - For N nodes in the network we have a $N \times N$ matrix
 - If node i and node j are connected, the element in row i and column j contains a 1
- Values of the elements (i, j) can also contain the **weight of the respective dependency**
 - The stronger the dependency the higher the weight



Interdependency Graphs

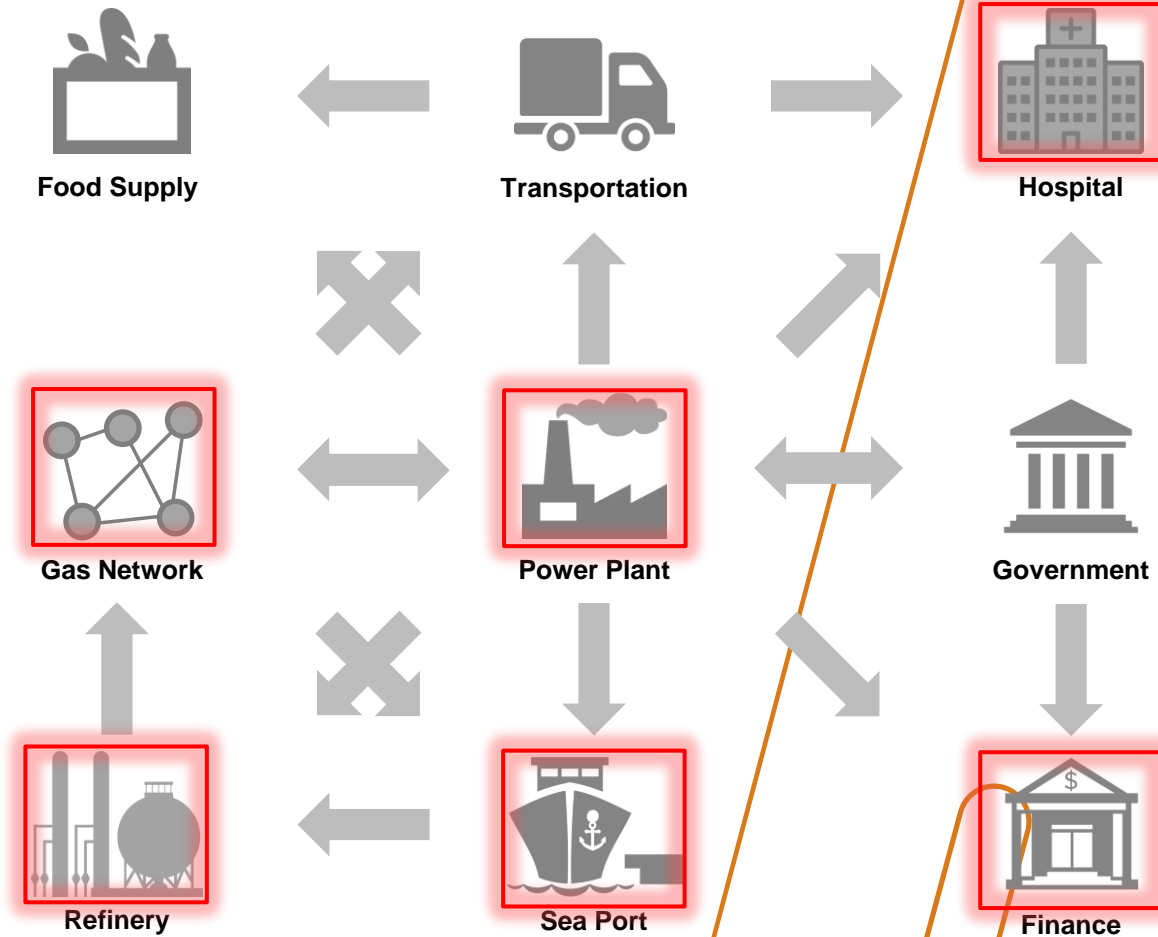
	P	T	W	H	F
P	0	0	1	0	0
T	0	0	1	0	0
W	0	0	0	1	1
H	0	0	0	0	0
F	0	0	0	0	0



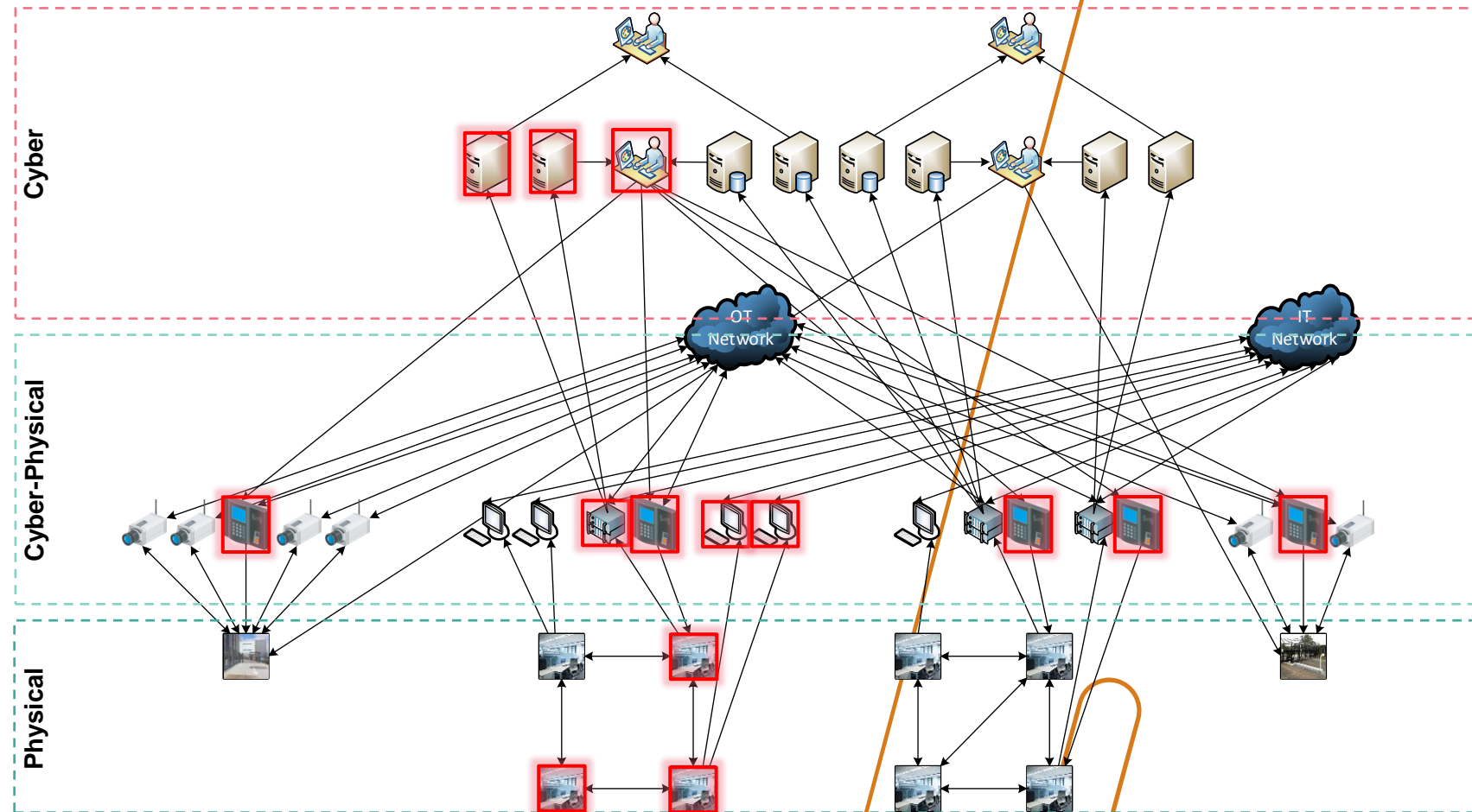
Cascading Effects

How can cascading effects be modelled and analysed?

Cascading Effects among Infrastructures



Cascading Effects among Infrastructures



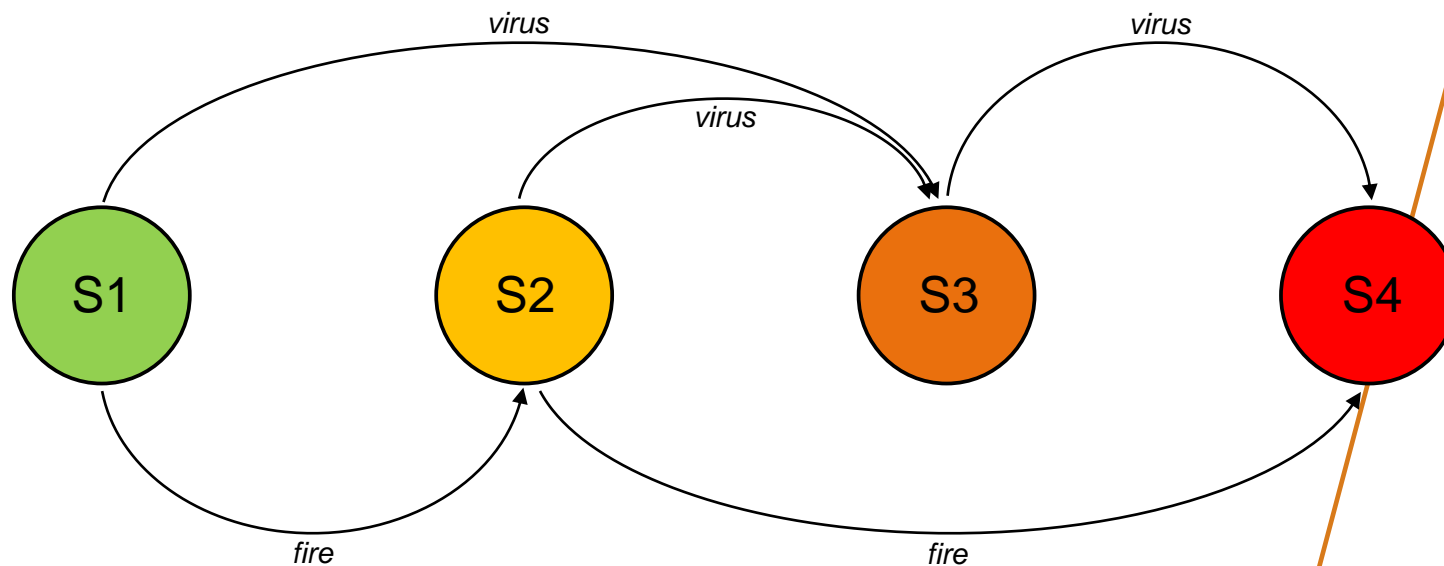
Modelling cascading effects

- For describing the state of a critical infrastructure, a binary system **might not be sufficient**
 - “fully operational” vs “complete breakdown”
- In real life, infrastructures can have **multiple different operational states**
 - Depending on available resources, production capacity, etc.
 - Operational states can **influence depending infrastructures** in various ways
- More **differentiated scale** to describe the operational status of a critical infrastructure will provide **better insight** into the evolution of the overall system

Modelling cascading effects

- One approach is to model the critical infrastructure as an **automaton or state machine**
- Number of **different operational states**
 - **Abstract representation** of the various states the infrastructure can be in
 - Detailed description can be formulated separately (e.g., internal specifications, etc.)
- Well-defined **transitions among those states**
 - Conversion from one state to another
 - State change is based on a specific input

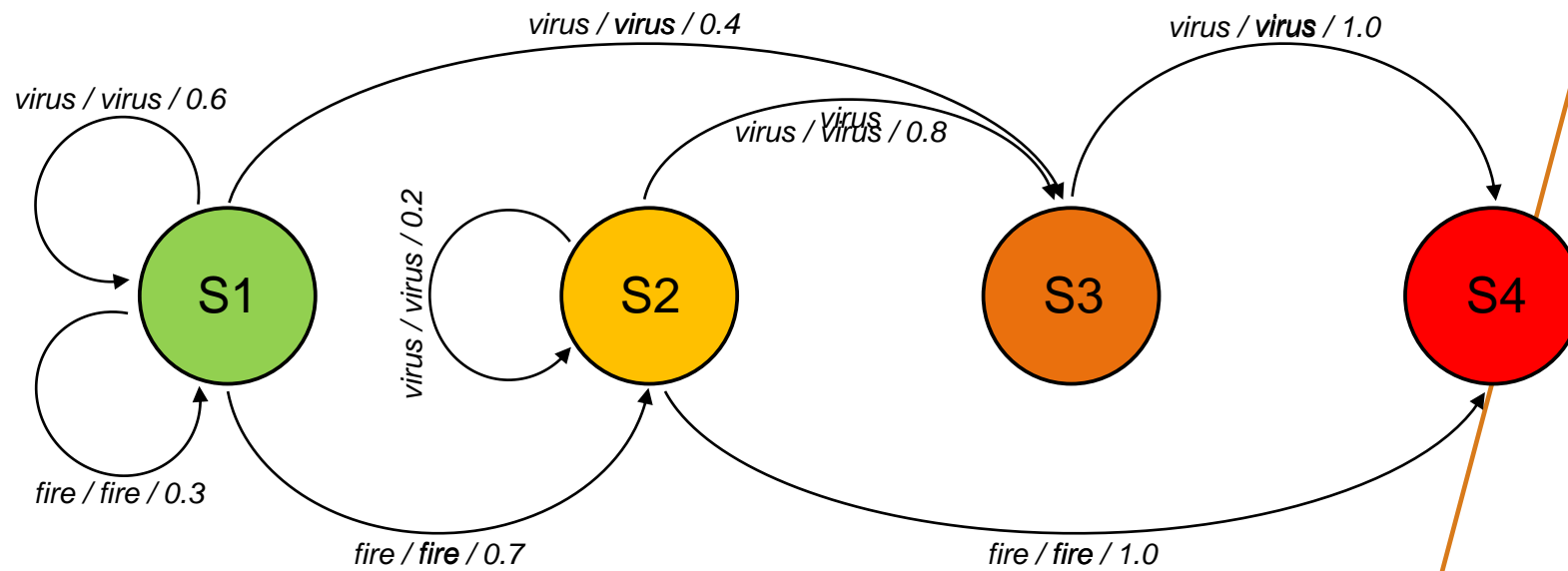
Modelling cascading effects



Modelling cascading effects

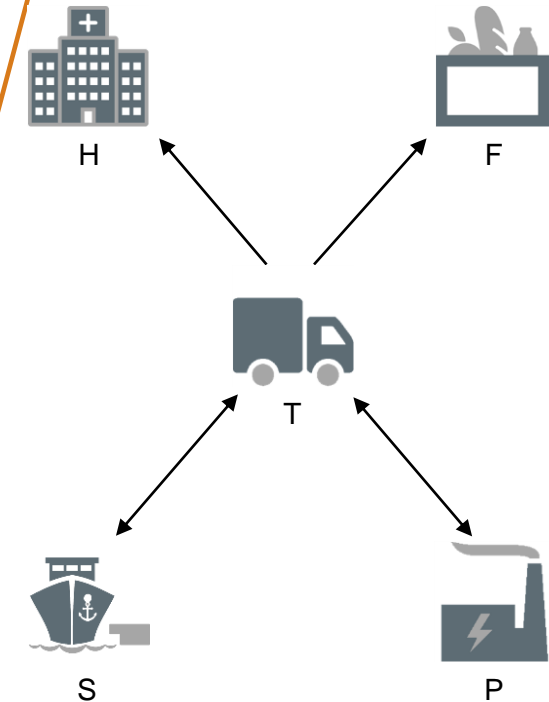
- Additional information is required to describe real-life scenarios
- States need to handle **input events** and also deliver **output events**
 - Triggering incident can originate somewhere else (i.e., external event)
 - State change can **trigger another event** (i.e., at another internal system)
- Infrastructures will react differently on distinct events
 - **Current state and triggering event** define the resulting state
- Transitions won't be **deterministic**
 - Real-life operation of infrastructures contains too much **uncertainty**
 - **Probability** needs to be included in the transitions

Modelling cascading effects

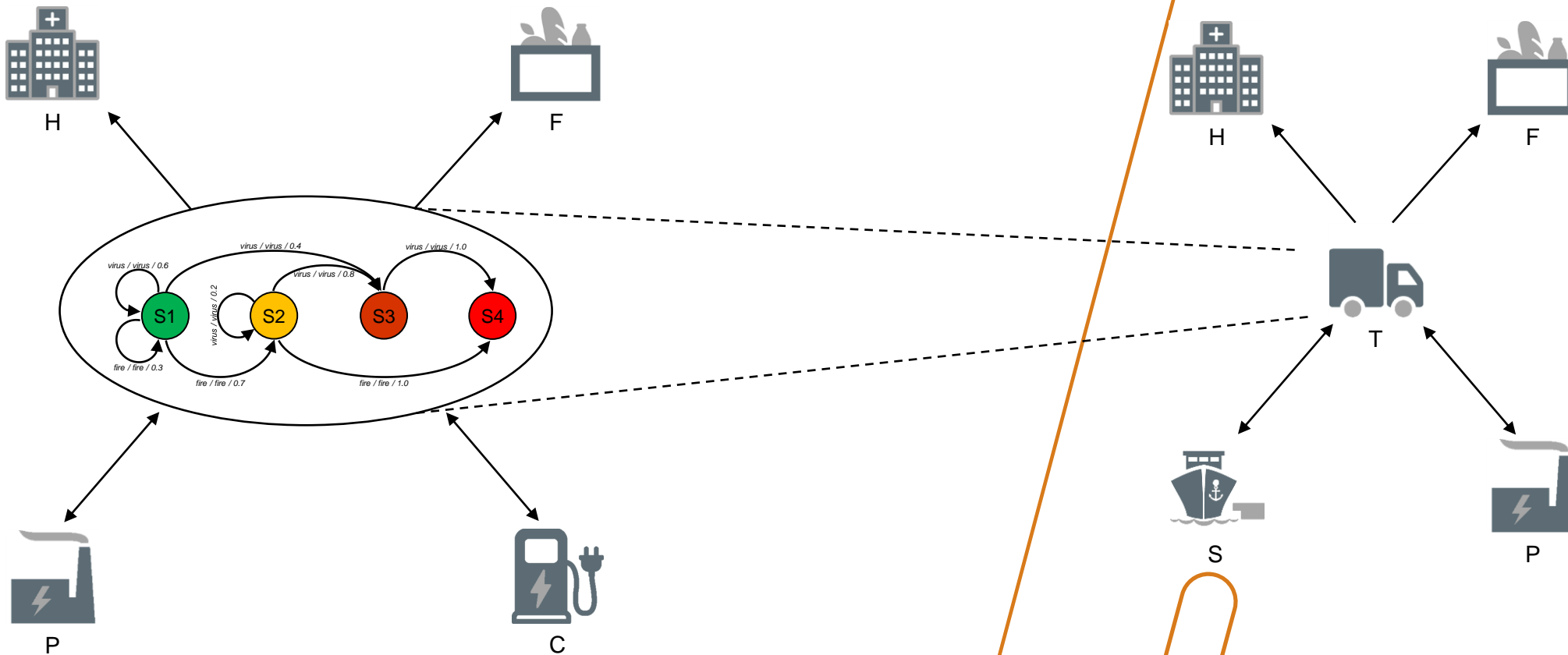


Modelling cascading effects

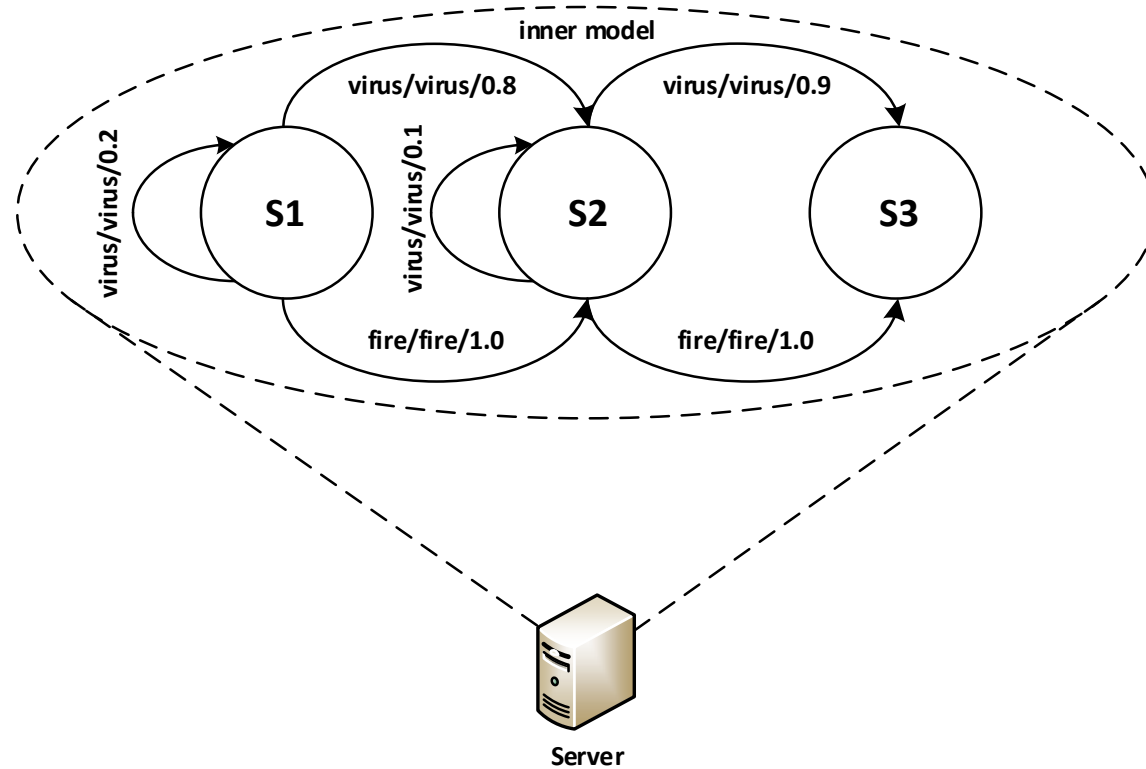
- Combine this more dynamic approach with the **interdependency graph**
- Each infrastructure can be in **one of several operational states**
 - Ranging from **“fully operational”** (“1”) to **“complete breakdown”** (“3”)
- Change of the operational state is based on
 - the **supplier infrastructures**
 - an **external event** (i.e., an incident)
- Change of the operational state happens with a **specific probability**



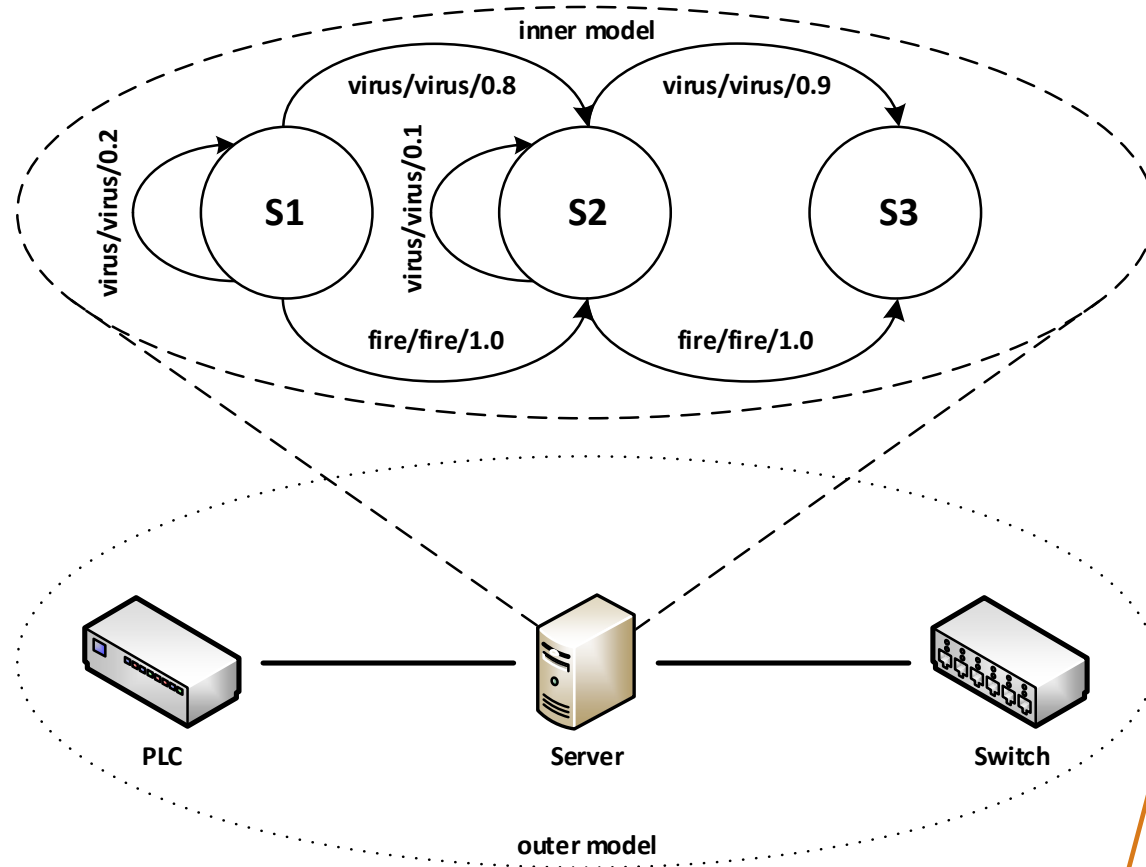
Modelling cascading effects



Modelling cascading effects



Modelling cascading effects



Simulating Cascading Effects

Simulation model describes the **evolution of the overall CI network**

- Stochastic risk model is instantiated
- **Large number of simulation runs** are carried out to evaluate a specific incident happening on one infrastructure

Incident/attack changes the **operational state of the target CI**

- Dependent CIs change their state, too (according to the probability distribution)
- Effects of the incident **propagate through the CI network**

Total impact is measured based on the **final state of all CIs** after the simulation has finished

Simulating Cascading Effects

Simulation model has been implemented in the SAURON project

Focus lies on the **physical and cyber assets** within maritime ports

- Model various assets in the physical and cyber domain
- Define the **operational states**
- Specify the **interdependencies** among them
- Define the **transition probabilities**

Scenarios with **incidents from different domains** can be simulated

- Physical incident affecting the cyber domain
- Cyber incident affecting the physical world

Simulating Cascading Effects

Tool records all **state changes** and the **final states** of each of the simulation runs

Simulation runs return an **overview on the system evolution**

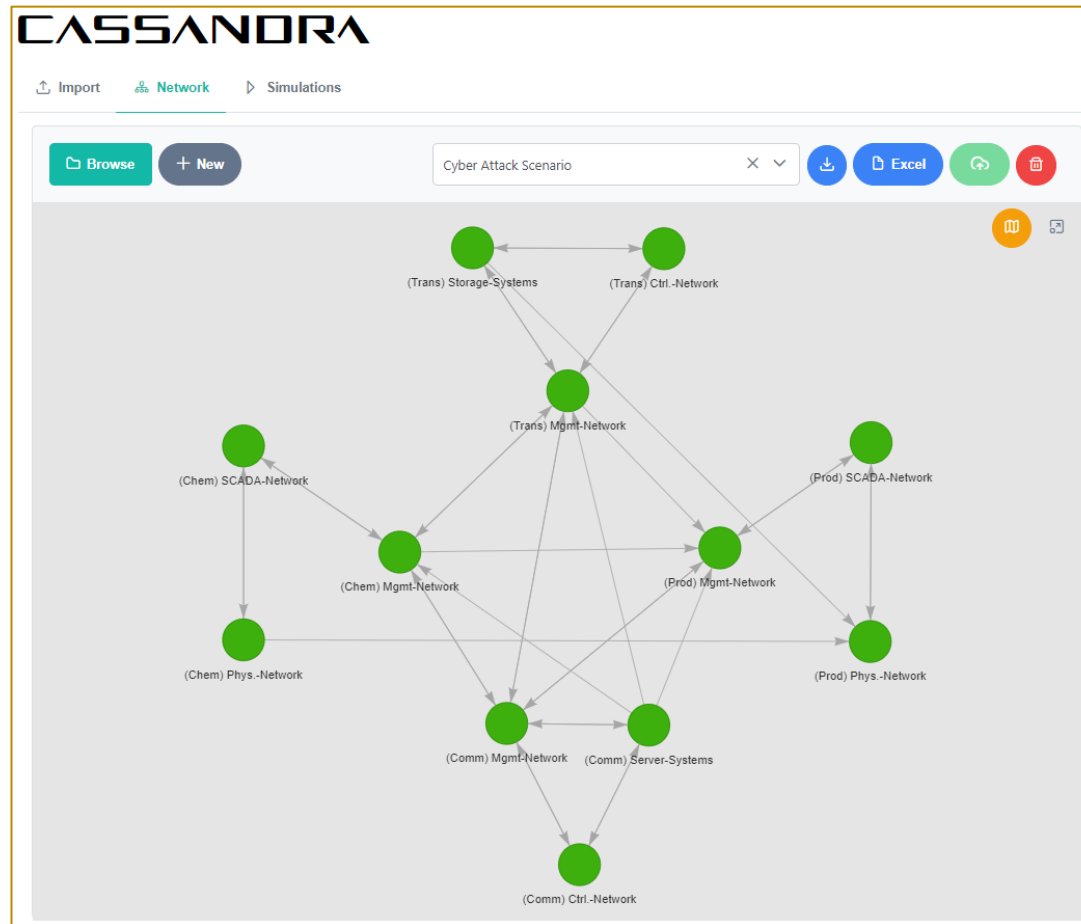
- Which asset has been “infected” in which step
- What is the new state of the asset
- Which asset caused the state change

Final states reflect the **overall impact of an incident** on the infrastructure

Different visualizations and reports can be generated

- **Average final state** of an asset
- **Average case scenario**
- **Worst case scenario**

Simulating Cascading Effects



Simulating Cascading Effects

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: 4.08

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

1 of 100

Example: Cascading Effects

How are cascading effects simulated in a realistic scenario?

Scenario “Port Infrastructure”

Physical Infrastructures

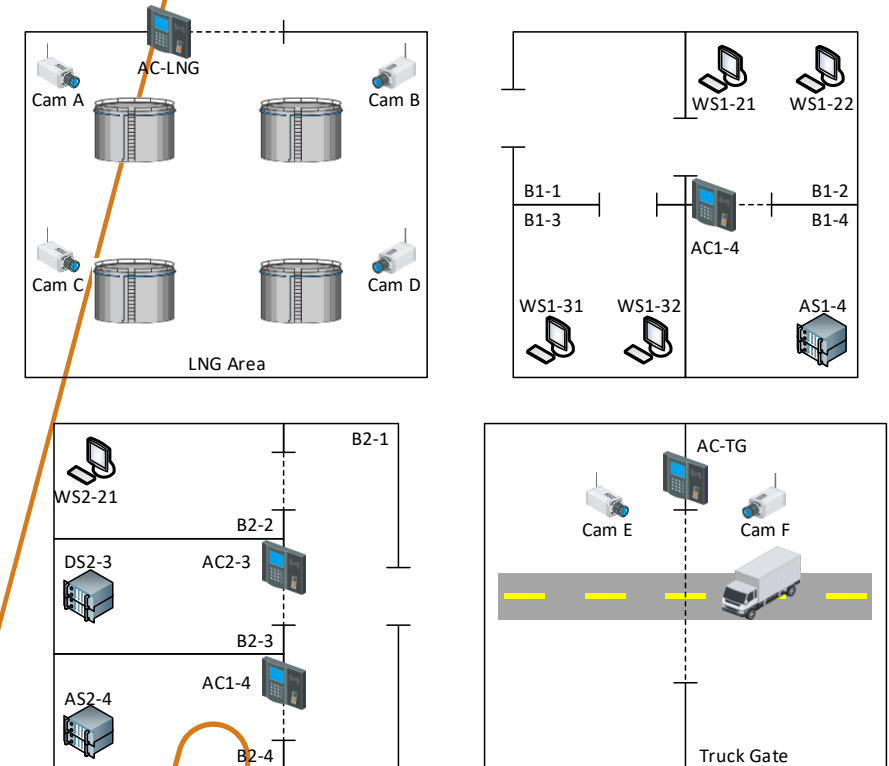
- LNG area and truck gate
- Two office buildings

Cyber-physical Infrastructures

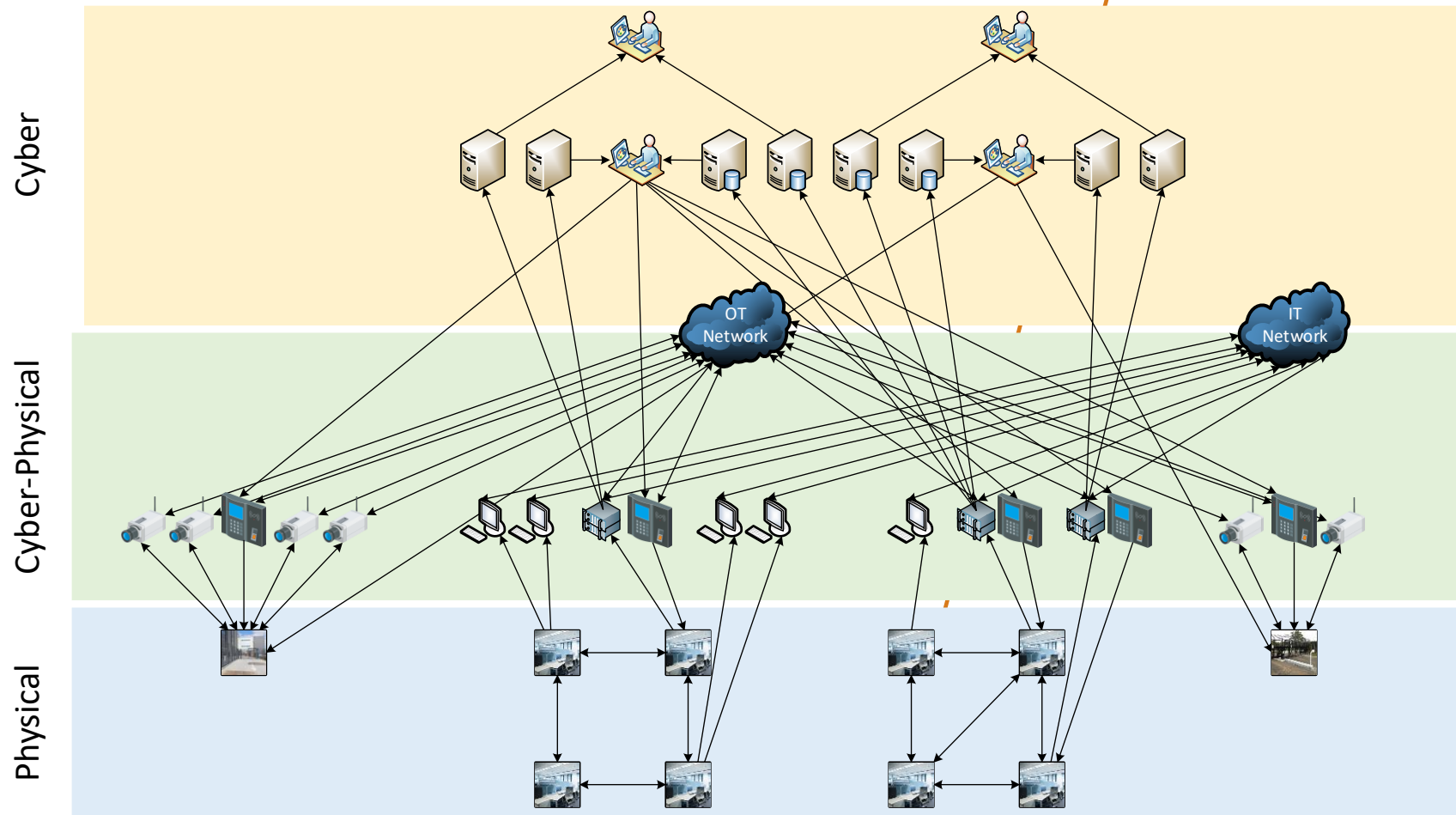
- Access control at specific gates
- Various surveillance cameras
- Three server racks
- Several work stations

Cyber Infrastructure

- Database and application servers
- Several important services

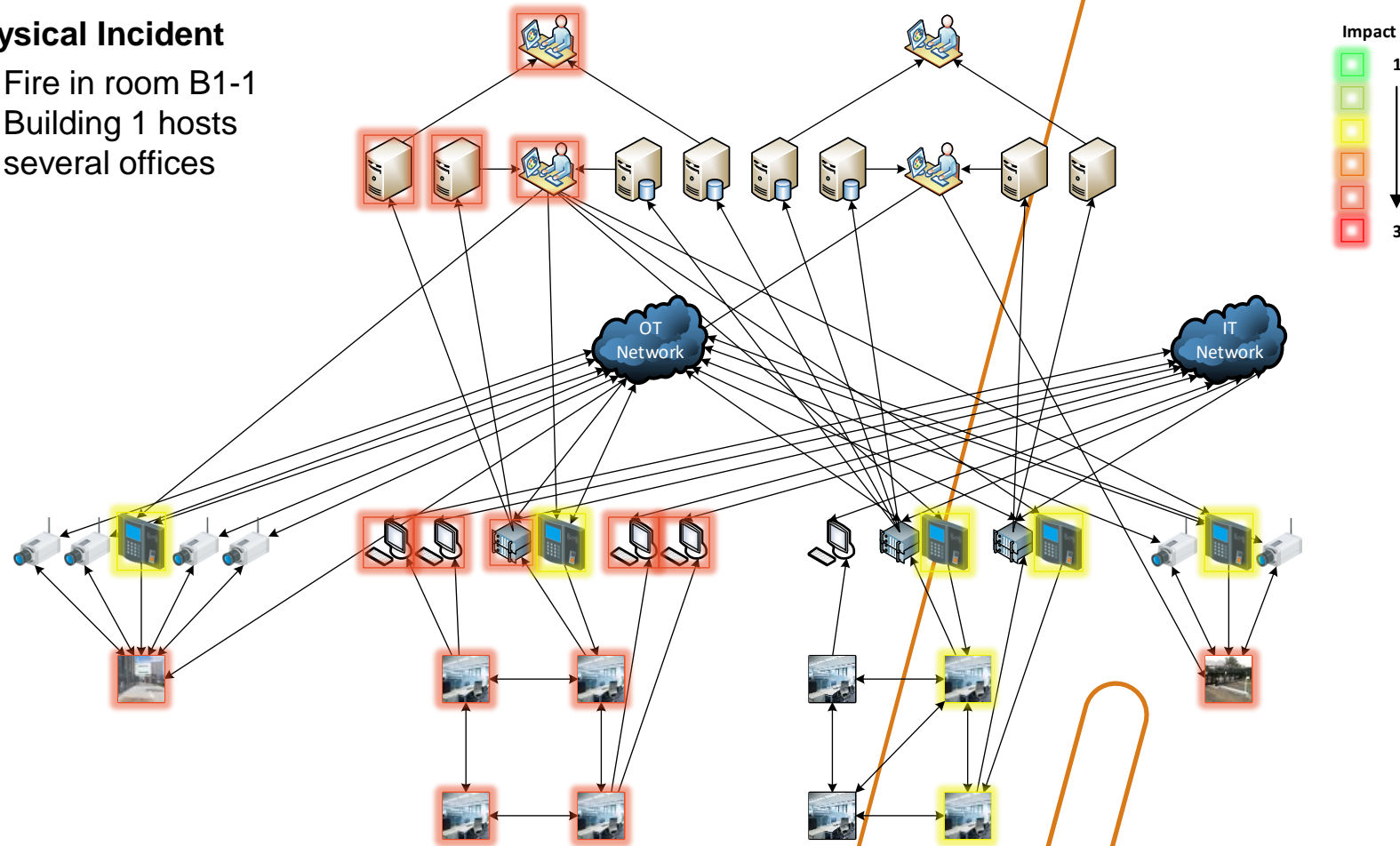


Scenario "Port Infrastructure"



Simulation Results

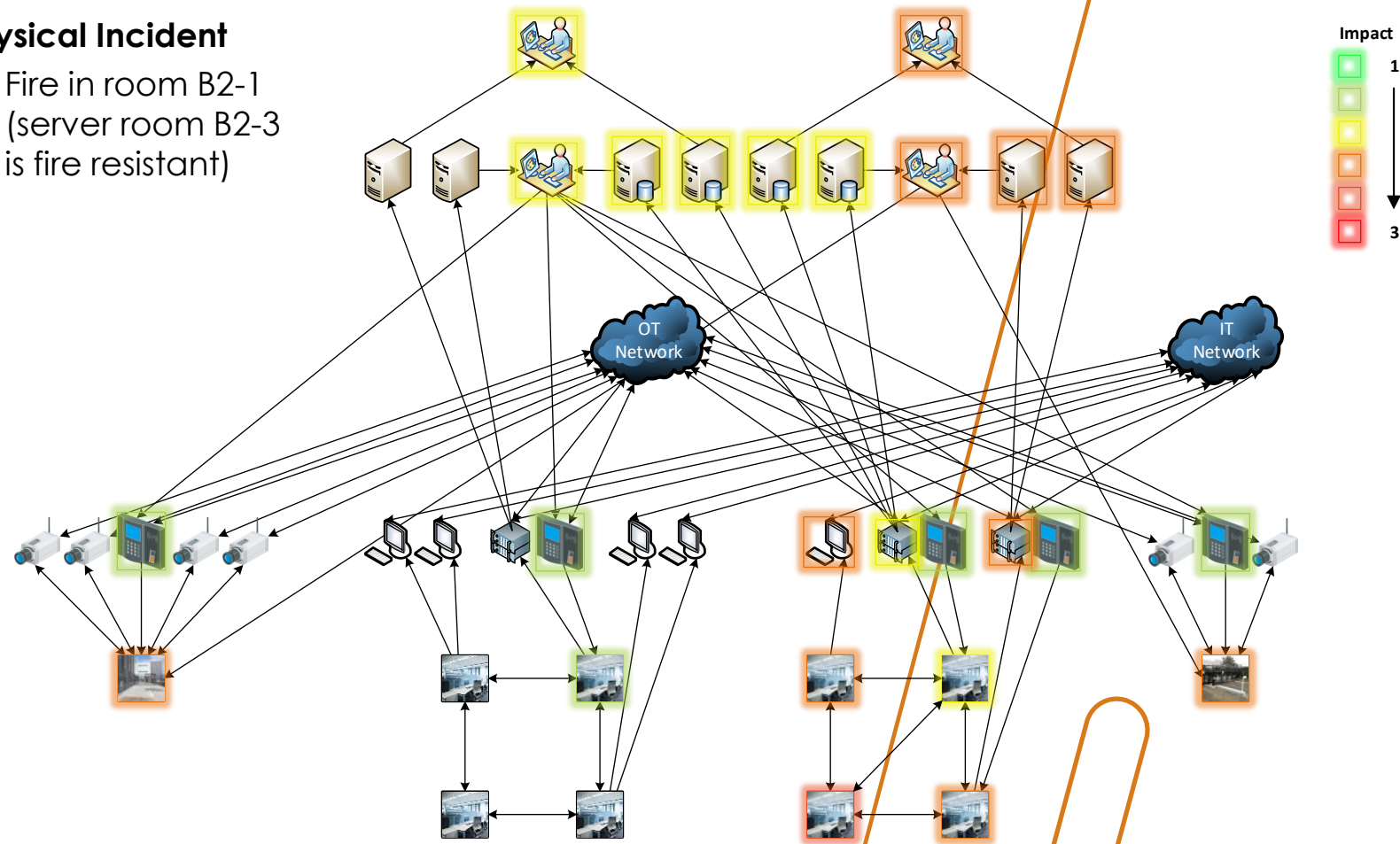
- **Physical Incident**
 - Fire in room B1-1
Building 1 hosts several offices



Simulation Results

- **Physical Incident**

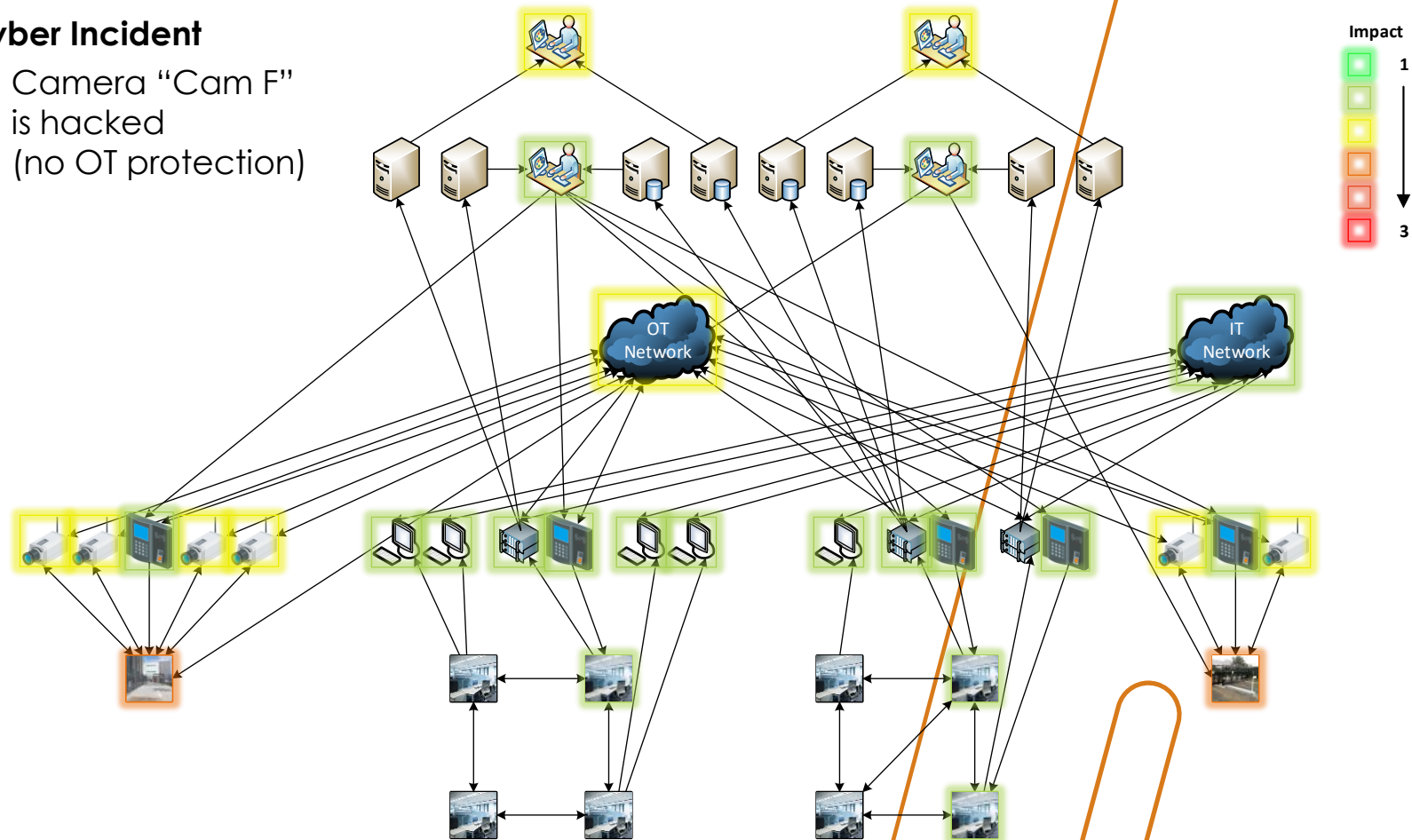
- Fire in room B2-1 (server room B2-3 is fire resistant)



Simulation Results

- **Cyber Incident**

- Camera "Cam F" is hacked (no OT protection)



Connect with CyberSecPro: How to register and other practical information

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

Thank you

Please send all questions to:

Stefan Schauer,

Stefan.Schauer@ait.ac.at

Abdelkader Shaaban

abdelkader.Shaaban@ait.ac.at