ATLANTIS

ATLANTIS approach to CI dependencies modelling and risk assessment

Webinar, 2.7.2025

Dr. Marko Gerbec, Jožef Stefan Institute, Slovenija
marko.gerbec@ijs.si

Institut "Jožef Stefan" Ljubljana, Slovenija

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Contents

- Why CI (inter)dependencies analysis & modelling? Approach
- CI(-to-CI) risk modelling approach
- Some example results
- Q&A

https://www.atlantis-horizon.eu/

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

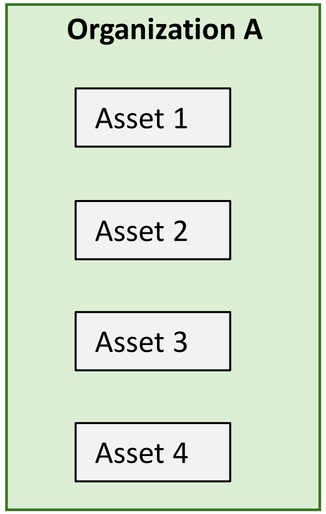
Dependencies modelling

Topics

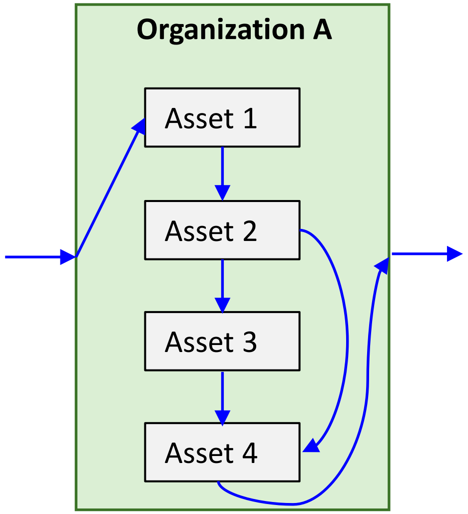
- CI – Critical Infrastructure
  - Composed of: assets that define CI and perform its function(s)
  - Assets (equipment, installations, …) are usually hierarchically organized (see e.g., ISO 14224:2016)
  - Assets are connected in order to perform CIs function(s)
- Group of CIs
  - That is how the society uses/depends on them – foundations!
  - A given CI is usually connected (dependent) in some way to other CIs
    - It may be a dependency at the input (suppliers)
    - It may be a dependency at the output (users)
    - **Consider complexity in a network of CIs and their assets**

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

What constitutes a complex organization?

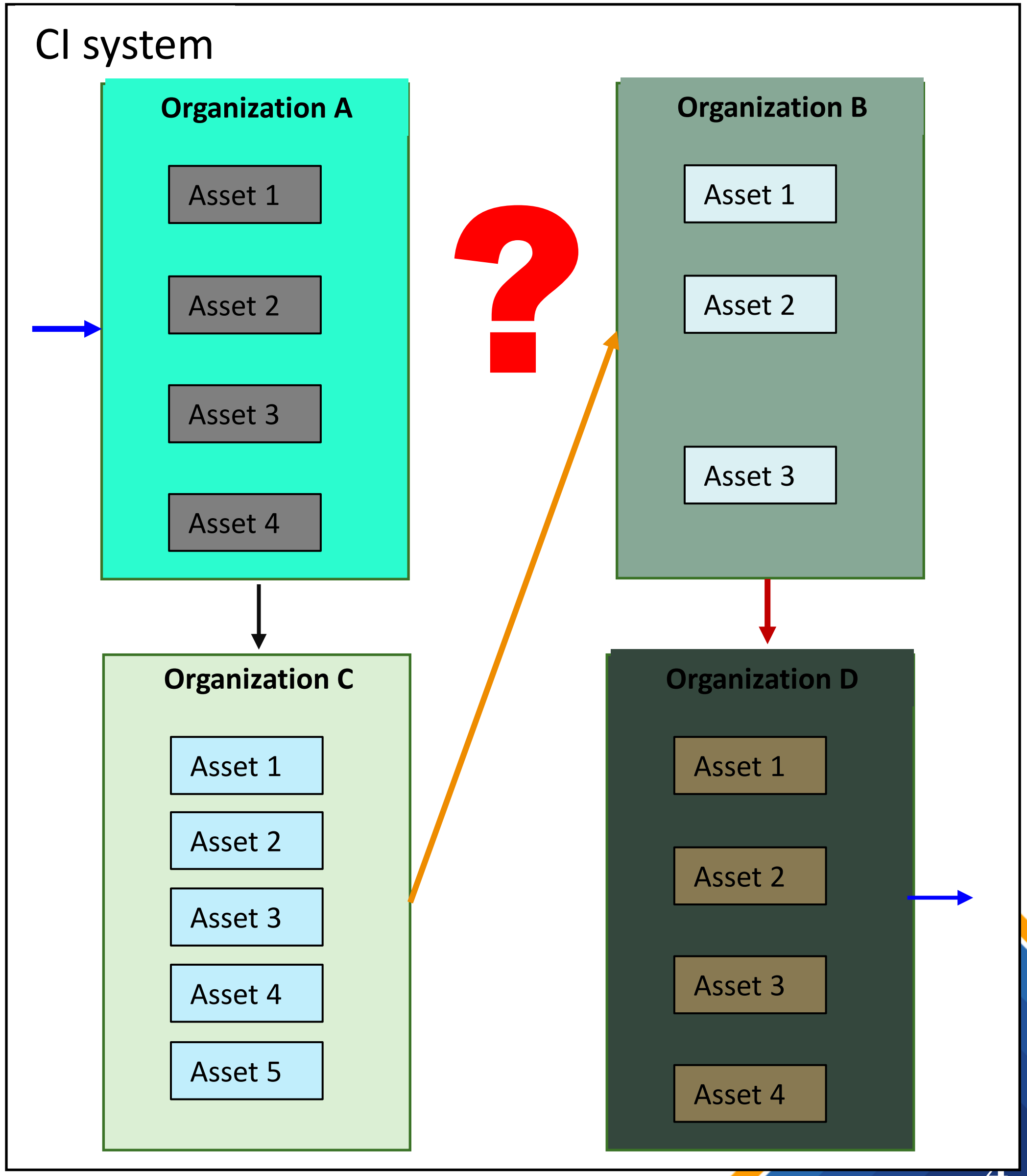


Organizations consist of assets (e.g., agents, technical systems) to realize their missions



How are assets related (dependent) while realizing their mission?

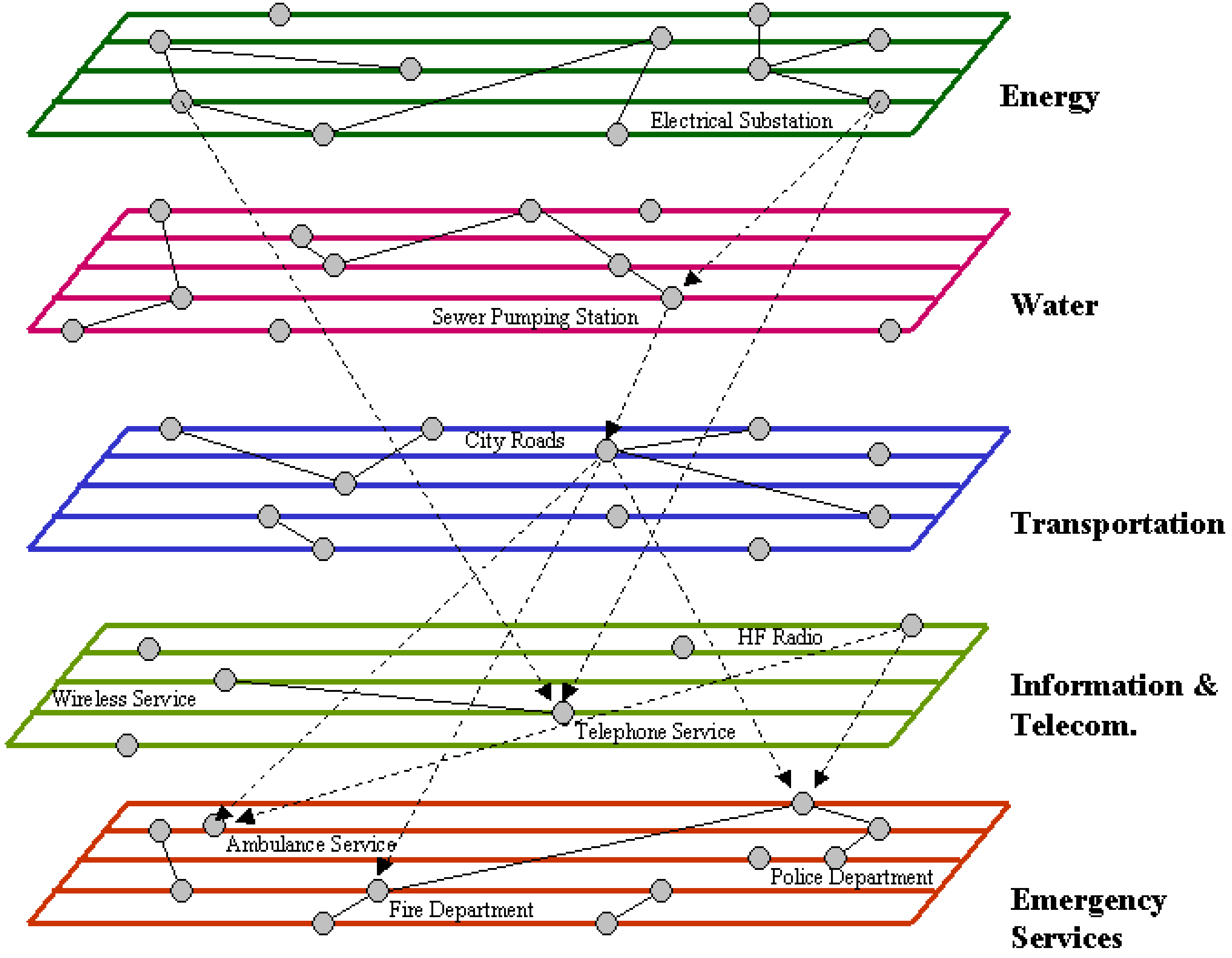
How to understand (analyze) complex system of organizations and their assets (relations, functions)?



This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073909.

It is more complex as it looks …

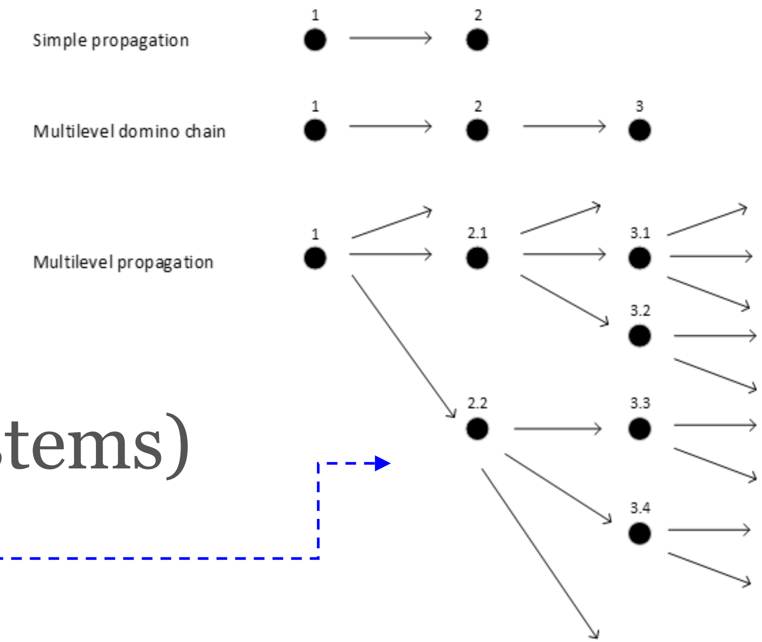
- Infrastructure interdependencies
- How many of them your CI uses?



This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073909.

Relations (interdependencies)

1) It is about the arrows on the previous slide
2) One needs a list of all assets/organizations
3) Need to find if <u>each</u> pair is somehow related
   - "Related": child is <u>dependent</u> on parent
   - Might be also bidirectional
4) List of relations can be very long (=complex systems)
5) Branching can develop (escalation)



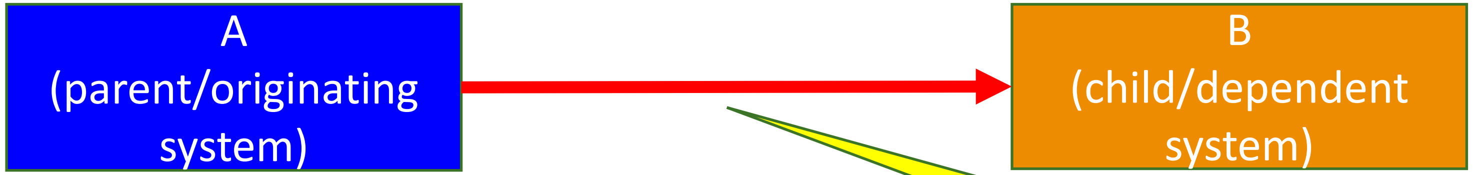
What is the purpose:

<u>thus we can map how the system (a set of CIs) logically works!</u>

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073909.

Types of arrows (interdependencies)

“the term interdependencies is conceptually simple; it means the connections among agents in different infrastructures in a general system of systems” (Rinaldi et al., 2001).



If A affects B:

- Some property of A has effect on B
- Which property of B will be affected?
- How strong the effect on B will be?
- Is it for sure?

Dimensions					
Infrastructure characteristics	State of operation	Types of interdependencies	Environment	Coupling and resp. behavior	Type of failure
Organizational Operational Temporal Spatial	Normal Repair/ Restoration Stressed/ Disrupted	Physical Cyber Logical Geographic Logical Functional Policy Shared Economic	Economic Legal Technical Social/Political	Adaptive Inflexible Loose/Tight Linear/Complex	Common cause Cascading Escalating

This project has received funding from the European Union’s Horizon Europe research and innovation programme under the grant agreement No 101073909.

Types of arrows (interdependencies)

	Type	Description	Potential overlap with
I	**Physical**	The state of one infrastructure system depends on the material, i.e., physical output of other systems. The prime example for these interdependencies is electricity loss and power outages.	V, VII, VIII
II	**Cyber**	The state of the considered infrastructure depends on information that is broadcasted through the information infrastructure system. Events caused by a disruption of telecommunication services belong to this class.	V, VII, VIII
III	**Geographic**	A geographically localized event might affect the state of infrastructure systems that are in proximity, such as the case of flooding events.	VI, VII, VIII
IV	**Logical**	This category summarizes cases where the state of one infrastructure system depends on another system via a mechanism that is not of a physical, cyber, or geographic type. For example, a disruption of public transport system might lead to congestion in other modes of transportation.	V-VIII
V	**Functional**	One might define functional interdependencies as those where the operation of one infrastructure system is necessary for the operation of another system. This might include physical or cyber interdependencies.	I-IV, VII, VIII
VI	**Policy**	Infrastructure systems might be connected due to policy or high-level decisions that directly affect several CIs. For instance, outages in power system might trigger a change of food and oil prices.	III, IV, VIII
VII	**Shared**	Physical components or activities are shared between several different CI systems (as opposed to being transmitted between them, as it is the case for physical interdependencies). For instance, the breakdown of a shared information service at a transportation hub might impact several CI systems.	I-V, VIII
VIII	**Economic**	Infrastructure systems interact with each other in a market (economic system) or provide services and goods to the same end users that in term determine the final demand and consumption of a particular commodity or service. Typically, economic systems also experience budget constraints that might introduce additional interdependencies. Economic interdependencies may also encapsulate interactions due to a shared regulatory environment, such as taxation and investments.	I-VIII

Adopted from Rinaldi et al., 2001

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073909.

Modelling starting points (1)

- CI-to-CI (inter)dependency modelling level can be:
  - Macro: only CI-to-CI dependencies are studied
  - Micro: one consider specific asset at a given CI and dependency to the specific asset at the other CI

- Macro level is quicker
- Micro level is much more informative, but much more work, necessary if risk assessment is the goal.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073909.

Modelling starting points (2)

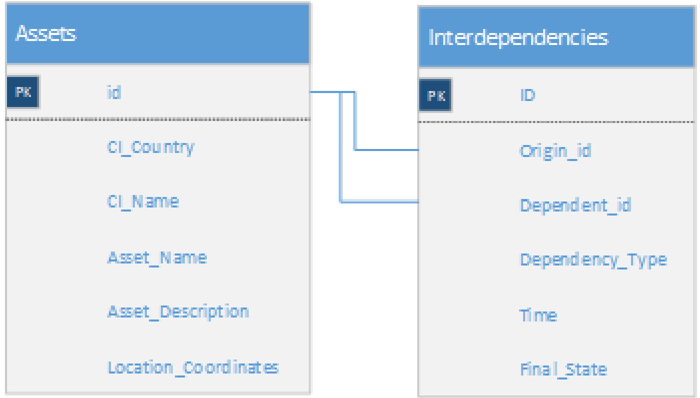
1. Define the modelling domain (which CIs to consider)
2. Define for each CI which assets are meaningful:
   - Assets/level should be detailed enough to reflect the operations
   - Do not get lost in details (issues: utilities, redundant systems, etc.)
3. For each CI & asset define also its basic data and explanations (somebody will read your analysis in some time …)
4. With a list of CI-assets study how the are they:
   - Related (dependent) one-to-one (type of dependency, choose the most important one).
   - If a parent fails, what happens to the child (severity)?
   - If a parent fails, how soon (time) the child will experience the severity?

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073909.

Assets and dependencies data model prepared

Data	Purpose
id	identifier of the asset (number)
Country	Country short name where the CI is located
CI	Critical infrastructure short name
Asset	Name of the CI's asset
Description	Explain the purpose of the asset
Latitude	Coordinates
Longitude	Coordinates

Data	Purpose
ID	Interdependency identifier (number)
OriginAssetName	Name of the origin asset in a case origin-dependent pair
DependentAssetName	Name of the dependent asset in a case origin-dependent pair
OriginID	Related id of the OriginAssetName
DependentID	Related id of the DependentAssetName
Category	Assigned dependency type (separate list)
Time	Assigned TimeCategory if origin fails
Final state	Text explanation on how to understand the dependent asset's final state



#	Time	Explanation
5	seconds	Dependent asset reaches final state within few seconds
4	minutes	Dependent asset reaches final state within few minutes
3	hours	Dependent asset reaches final state within hours
2	days	Dependent asset reaches final state within days
1	weeks	Dependent asset reaches final state within weeks

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073909.

Examples (we compiled data in MS Excel)

id	Country	CI	Asset Title	Description	Latitude	Longitude
1	SLO	SZ	CVP	CVP - Traffic management centre (Center vodenja prometa - CVP) (including data and communications centre, etc.)	45.55458	13.76598
2	SLO	SZ	Diesel	Diesel - Backup Diesel generator for elecrical power at CVP	…	…
3	SLO	SZ	Main tracks	Main tracks - Main group of the railway tracks at Koper cargo station		
4	SLO	SZ	Switch 501	Switch 501 - railway switch 501 to acces the industrial tracks of Petrol's TIS site		
5	SLO	SZ	SNEV	SNEV - Stable equipment for electrical drive supply at Koper cargo station (Stabilne naprave električne vleke - SNEV)		
6	SLO	SZ	SVN	SVN - Entry/Exit signal safety devices at cargo station Koper (Uvozne/izvozne Signalno varnostne naprave - SVN)		
7	SLO	SZ	Transformer	Transformer - Transformer station delivering electrical power for cargo station Koper		
8	SLO	ELES	ELES grid	ELES - national electrical power grid operator		
…						
28	SLO	TS	BON	BON - Backbone Optical Network		
29	SLO	TS	EN	EN - Electrical power suppy stations (from ELES power lines)		

"Id" is used further

Allows presentation on the map

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073909.

Example dependency mapping

ID	OriginID	DependentID	Category	Time	Final state
1	2	1	Physical	seconds	Completely non operational
2	3	1	Functional	seconds	Almost completely non operational
3	6	1	Functional	seconds	Almost completely non operational
4	7	1	Physical	minutes	Completely non operational
5	7	2	Logical	seconds	Diesel takes over
6	1	3	Functional	seconds	Completely non operational
7	2	3	Functional	seconds	Completely non operational
8	4	3	Shared	seconds	No access to the Petrol's tracks (passage).
…	…	…			

"Id"s of the assets

It is good practice to actually enter the asset name and use Lookup() function to assign its "id"

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073909.

How to approach dependencies mapping?

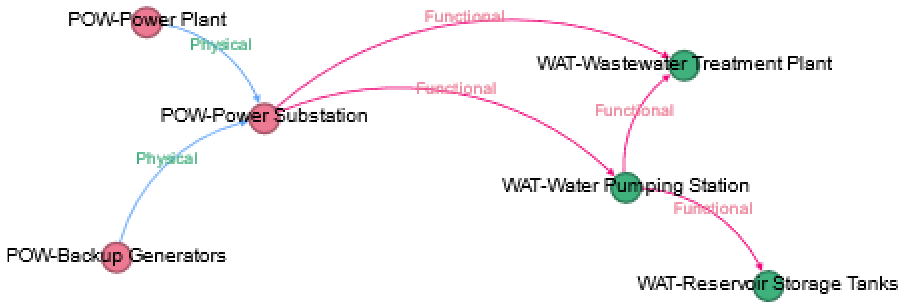
Filling up the dependencies table on the previous slide might be error prone (some dependencies forgotten, double counting, etc. ?).
Simple intuitive solution (but extra work) is to first transpose list of assets to the matrix and assign one-to-one dependency type in cells – see example:

		Origins							
		TARO	TARA	SM	PT	IT	Ops. Dpt.	LUR PCC	SZ Main tracks
Dependent	TARO		Logical		Physical	Cyber	Functional		
	TARA	Logical			Physical	Cyber	Functional		Shared
	SM				Physical	Cyber	Functional		
	PT	Logical	Logical	Physical		Cyber	Functional		
	IT								
	Ops. Dpt.	Functional	Functional	Functional	Physical	Cyber		Logical	
	LUR PCC						Logical		
	SZ Main tracks		Shared						

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073909.

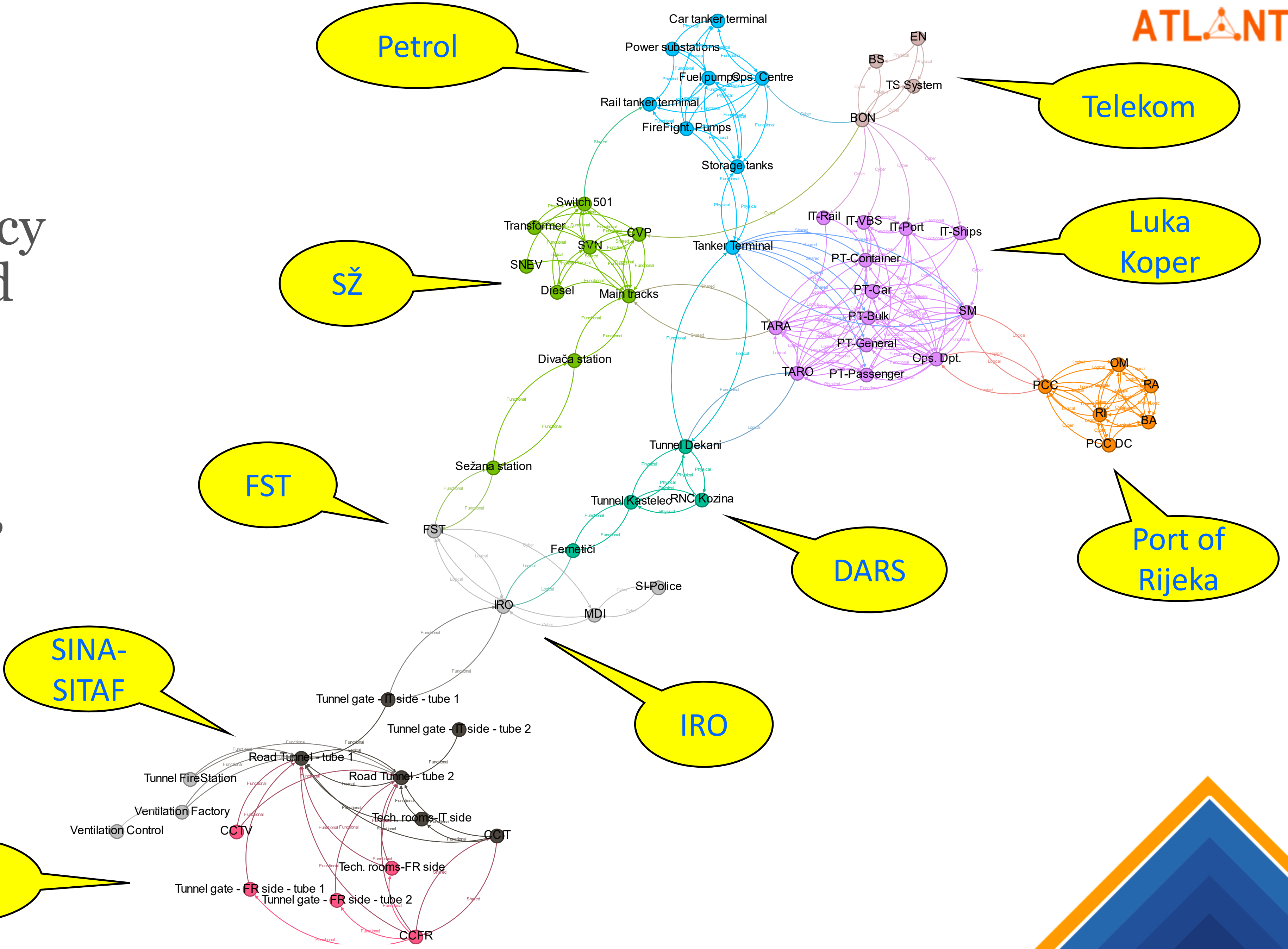
Graphical results and checks

- It is a good idea to check for logical errors in relations using graphs
- Tables can be easily imported in graphing free tools like Grafana, Gephi, etc.



This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073909.

- Example of interdependency graph prepared within ATLANTIS LSP#1 pilot (SLO, CRO, IT, FR)



This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073909.

Why ATLANTIS Risk Assessment method?

- CIs are exposed to diverse hazards/threats
  - NaTech, industrial accidents, attacks (physical, cyber, hybrid)
- Conventional RA considers only an individual CI and its parts
- **There is a need:** to understand relations among CIs, CI sectors, national and international levels
- Previous EU projects (SmartResilience, DEFENDER, InfraStress, ...) set the foundations.
- ATLANTIS offers an approch to CI-CI risk evaluation

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Methods used

- ATLANTIS approach:
  1. Identify critical parts of each CI
  2. Identify (inter)dependencies among a set of CIs
  3. Identify sources of hazards/threats (→risks)
  4. Develop technology for data processing for decision support

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

6 Methodological steps

Step 1: Define the Scenario

Step 2: Identify Key Assets

Step 3: Identify Interdependencies

Step 4: Analyse Threats

Step 5: Analyse Impacts

Step 6: Calculate Risk Scores

- **Previous analyses**
- CI management involvement
- Actual exposure
- Types of hazards/ threats

- Severity level criteria
- Relevance for CI
- Relevance for other CIs

- Sources for CI
- CI is a source for …?

(see next slides)

- Probabilities analysis:
  - Hazard occurence
  - Hazard→Failure
  - Failure→Consequences

- Analysis of the severity of the consequences
- 7 evaluation categories

- Risk=[probability]× [consequences evalu.]
- Risk interpretation

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Step 1: Define the scenario

Hazard/threat must impact at least one CI operator, potentially other CI(s).

For each CI involved in each stage, we analyse the following:

- What happened, and what caused this step?
- What actions are being taken by CIs in response?
- What cascading effects can be observed, and what could happen next?

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Step 2: Identify Key Assets

- Key assets are directly impacted by identified hazard/threat, or indirectly via interdependencies.
- For each asset we provide brief description and analysis:
  - What is the role and purpose of this asset?
  - What inputs does the asset require to operate?
  - What does the asset provide to support other assets?
- This assures consistent consideration of assets and analysis of dependences (see also tables at the slides 10 and 11).

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Step 3: Identify Interdependencies

- The interdependency analysis for the modelled domain of CIs is performed as shown on slides 3 to 14.
- In addition, possible alternatives (spares) for failed/incapacitated assets and utility systems are considered.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Step 4: Analyse Threats

Consist of 3 sub.-steps:

1. Linking sensor data to asset states (e.g. working/not working).
2. Asset's states are linked to the failed state(s) cause(s) (e.g., "not working" to "no power")
   - Asset's states probabilities are assigned based on the available historical data
3. Causes of failures are related to hazard/threat categories (=probabilities can differ!)

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Adopted threat/hazard categories

Threat/hazard category	Brief description
Technology-Human-Organizational (THO)	Unintentional industrial site failures due to human error, technological faults, or hazardous substance releases. May include nuclear and radiological events.
NaTech and climate-related	Natural hazards (e.g., floods) that trigger failures in CI due to weakness in THO measures. Also includes extreme weather phenomena linked to climate change.
Physical attack	Intentional human-caused disruption, such as unauthorised access or direct attacks on CI sites (e.g., terrorist attack, sabotage).
Cyber-attack	Malicious cyber intrusions or conditions that lead to asset loss or operational failures, including hacking, malware, data breaches, and system disruptions.
Technology trends related	Emerging disruptive technologies that could create vulnerabilities or security concerns within CI systems.
Foreign Direct Investments (FDI)	Security risks associated with foreign ownership or investment in CI, including potential denial of access, espionage, and technology leakage.
Critical supplies (non-EU)	Risks related to supply chain dependencies on non-EU countries, potentially causing disruptions in essential materials, technology, or expertise.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Example of the table at this stage

Note that we do not consider "Normal state"

Asset (CI)	Sensor Value	Value Interpretation	Origin Asset (CI)	Asset State	State Prob.	Event	Threat Category	Threat Prob.
Power Plant (POW)	Working	Normal state	/	Normal	/	Normal	/	/
	Not working	Power failure	External	Electricity unavailable	100%	Threat	THO	70%
						Threat	NaTech	30%
Power Substation (POW)	Working	Normal state	/	Normal	/	Normal	/	/
	Not working	Power disruption	Power Plant (POW)	Electricity unavailable	90%	Threat	THO	100%
	Not working	Power disruption	Backup Generators (POW)	Backup power failure	10%	Threat	Physical attack	100%

Decision was that the sum of ALL asset's failed state probabilities is 1 (100 %)

All threat cat. sum up to the 100 % for a given state.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

ATLANTIS

Step 5: Analyse Impacts

- In this step, we analyse the potential impacts of the CI failures across multiple impact categories.
- The structured approach, adapted from Bennett, 2007, ensures that all relevant categories are semi-quantified, aggregated, and weighted to appropriately reflect the scenario's real-world implications.
- For each failure scenario (i.e., for each row), we score impacts using a scoring scale from 0 to 4 across the categories and scoring criteria:

This project has received funding from the European Union’s Horizon Europe research and innovation programme under the grant agreement No 101073878.

Impact Category	Score and criteria
1. People Exposed: **The number of individuals affected.**	0: None exposed. 1: 1-50 people exposed. 2: 51-250 people exposed. 3: 251-1000 people exposed. 4: 1001+ people exposed.
2. Economic Impact (Repair or replacement costs): **The financial burden of restoring services.**	0: No significant economic effect. 1: Restoring cost is less than 250.000 €. 2: Restoring cost is between 250.000 and 1.000.000 € 3: Restoring cost is between 1.000.000 and 10.000.000 €. 4: Restoring cost is greater than 10.000.000 €.
3. Economic Impact (Contribution to economy): **Wider economic consequences.**	0: No significant economic effect. 1: Impact on the individual critical asset's profitability is >10%. 2: Impact on the organisation's profitability is >10%. 3: Impact on the regional economy. 4: Impact on the national economy.
4. Business or Service Interruption: **Duration and severity of operational downtime.**	0: Critical assets could operate with minimal operational changes or repair. 1: Critical assets could partially operate. 2: Critical asset is shut down or unable to operate for <6 months. 3: Critical asset is shut down or unable to operate for >6 months. 4: Critical asset is not expected to be restored.
5. Interdependencies: **Effects on interconnected infrastructure.**	0: No effect on the critical asset's normal operations. 1: Critical asset is a stand-alone facility and is not interdependent on other assets; adverse effects would not extend beyond this single asset. 2: Critical asset is part of a larger system; however, adverse effects would not extend beyond this single asset 3: Critical asset is part of a larger system, and at least one other asset depends on its outputs. 4: Critical asset is part of a larger system, and many other assets depend on its outputs.
6. Criticality: **The importance of the asset in maintaining essential services.**	0: No adverse effect. 1: Minor adverse effects would occur, limited to a local environment. 2: Significant adverse effects would occur, limited to a local environment 3: Significant adverse effects would occur in a wider environment. 4: Significant adverse effects would occur nationally or worldwide.
7. Environmental Impact: **Potential damage to water, air, soil, and biodiversity.**	0: None. 1: Limited damage. 2: Short-term damage to limited extension of surrounding environment. 3: Long-term damage to limited extension of surrounding environment or short-term damage to significant extension of surrounding environment. 4: Permanent or long-term damage to significant extension of surrounding environment.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Use of weights

- In addition to Bennett, 2007, we apply weights per impact category that should be applied at the CI level:

Weight	Grade	Description
1	Low priority	The category has minimal influence on risk mitigation decisions.
2	Moderate priority	The category is important but balanced with other high-priority factors.
3	High priority	This category is a critical factor in risk mitigation; failure would have severe implications on the business process.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Use of weights

Calculations:

TI = Total impact

$$TI = \sum_{\substack{Sum\ Across\ all \\ Impact\ Categories}} (Category\ Weight \times Impact\ Score)$$

TI_N = Total impact normalized [0,1]

$$TI_N = \frac{TI}{\sum_{\substack{For\ all \\ Impact \\ Categories}} Category\ Weight \times 4}$$

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Step 6: Calculate Risk Scores

- Final *Risk Score* is calculated considering total normalized impact and conditional probabilities of the specific asset's state.
- Risk value is between [0-100]

$$Risk\ Score = State\ Probability \times Threat\ Probability \times TI_N \times 100$$

- Risk Score is presented as percentage.
- Possible risk levels (interpretation) on *Risk Score* are:

  <25%: Low Risk
  25-50%: Medium Risk
  50-75%: High Risk
  >75%: Critical Risk

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

ATLANTIS

Example of simplified view of the overall table

Asset	Asset State	State Prob.	Threat Category	Threat Prob.	People	Repair Costs	Economic Loss	Disruptions	Interdependencies	Criticality	Environment	(Normalised, Weighted) Total Impact
Power Plant	Normal	100%	/	100%	0	0	0	0	0	0	0	0.00
	Electricity unavailable	100%	THO	70%	3	4	4	4	3	4	2	0.88
			NaTech and Climate Change	30%	2	3	3	3	3	3	3	0.70
Power Substation	Normal	100%	/	100%	0	0	0	0	0	0	0	0.00
	Electricity unavailable	90%	THO	100%	3	4	3	4	4	4	1	0.88
	Backup power failure	10%	Physical Attack	100%	1	2	2	3	2	2	0	0.46
Backup Generators	Normal	100%	/	100%	0	0	0	0	0	0	0	0.00
	Physical damage	80%	NaTech and Climate Change	95%	2	3	2	3	2	3	2	0.63
			Physical Attack	5%	2	3	2	3	2	3	2	0.63
	Fuel supply disruption	20%	THO	100%	1	2	1	2	2	2	1	0.41

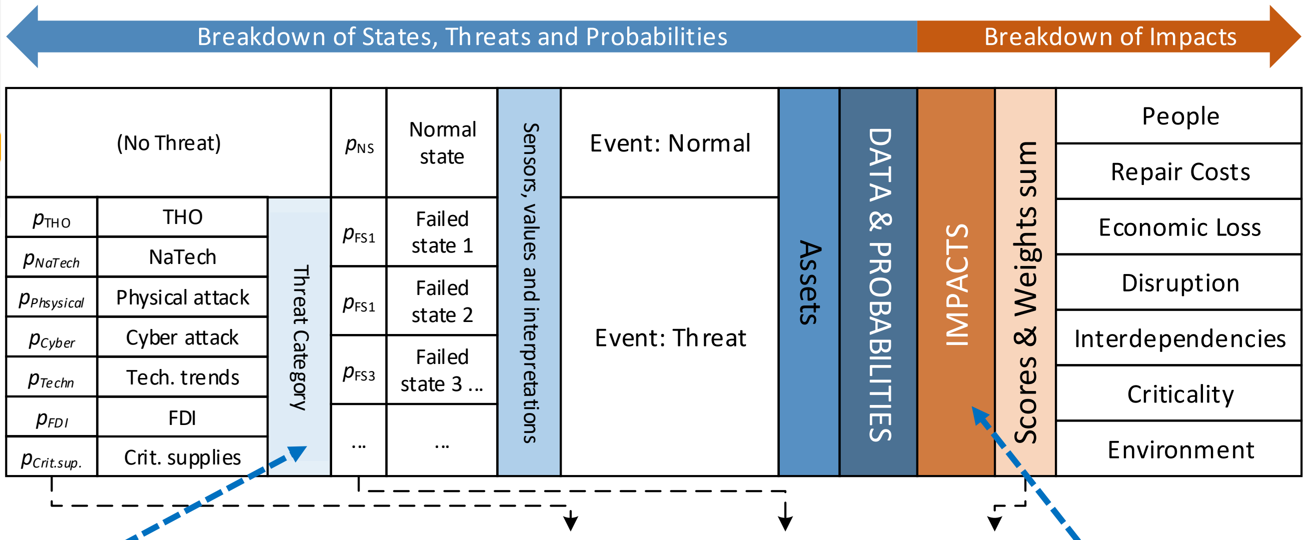
This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Example of simplified view of the overall table

Asset	Asset State	State Prob.	Threat Category	Threat Prob.	Impact Score	Risk Score	Risk Level
Power Plant	Normal	100%	/	100%	0.00	0.00	Low Risk
	Electricity unavailable	100%	THO	70%	0.88	61.25	High Risk
			NaTech and Climate Change	30%	0.70	6.27	Low Risk
Power Substation	Normal	100%	/	100%	0.00	0.00	Low Risk
	Electricity unavailable	90%	THO	100%	0.88	78.75	Critical Risk
	Backup power failure	10%	Physical Attack	100%	0.46	4.64	Low Risk
Backup Generators	Normal	100%	/	100%	0.00	0.00	Low Risk
	Physical damage	80%	NaTech and Climate Change	95%	0.63	47.50	Medium Risk
			Physical Attack	5%	0.63	2.50	Low Risk
	Fuel supply disruption	20%	THO	100%	0.41	8.21	Low Risk

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Overall model, considering categories



$$Risk\ Score = p_{Threat\ Category} \times p_{Failed\ state} \times Total\ Impact_N \times 100$$

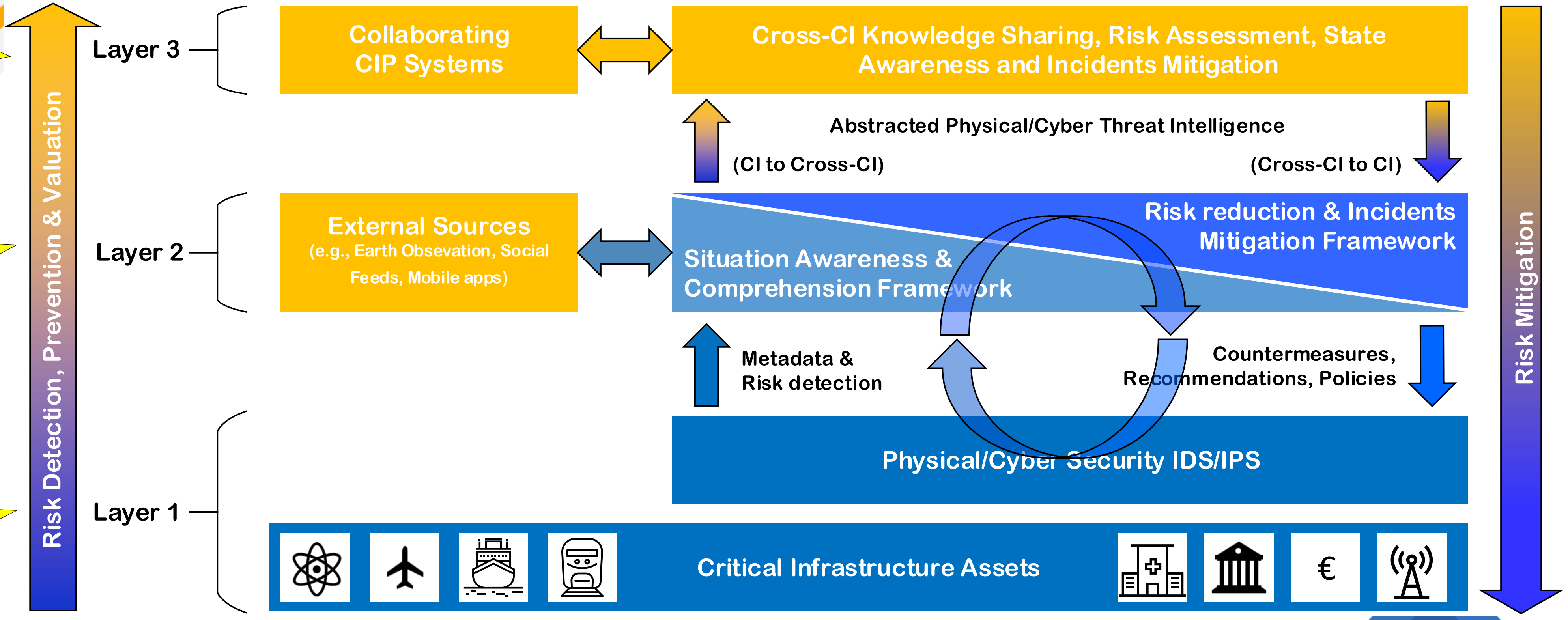
Threat/hazard category
Technology-Human-Organizational (THO)
NaTech and climate-related
Physical attack
Cyber-attack
Technology trends related
Foreign Direct Investments (FDI)
Critical supplies (non-EU)

Impact Category	Topic (0-4 score applies)
1. People Exposed:	The number of individuals affected.
2. Economic Impact (Repair or replacement costs):	The financial burden of restoring services.
3. Economic Impact (Contribution to economy):	Wider economic consequences.
4. Business or Service Interruption:	Duration and severity of operational downtime.
5. Interdependencies:	Effects on interconnected infrastructure.
6. Criticality:	The importance of the asset in maintaining essential services.
7. Environmental Impact:	Potential damage to water, air, soil, and biodiversity.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Information processing – source: sensors

- Joint "CIs group" information sharing system
- CI's local incident response system
- CI's system of incident detection



This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Main co-Contributors

- Jolanda Modic, ICS
- Artemis Voulkidis, Synelixis
- Denis Čaleta, ICS
- Gabriele Giunta, ENG

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

References used

- Rinaldi M, Peerenboom JP, Kelly T (2001). Identifying, understanding and analysing crit-ical infrastructure interdependencies. IEEE Control System Magazine, 11–25. https://doi.org/10.1109/37.969131
- Brian T. Bennett, 2007. Understanding, Assessing, and Responding to Terrorism - Pro-tecting Critical Infrastructure and Personnel; Wiley: Hoboken, USA. ISBN: 978-1-119-23781-5.
- Faisal Khan, Samith Rathnayaka, Salim Ahmed, 2015. Methods and models in process safety and risk management: Past, present and future. Process Safety and Environmental Protection. 98, 116-147. https://doi.org/10.1016/j.psep.2015.07.005
- CCPS, 2002. Guidelines for analyzing and managing the security vulnerabilities of fixed chemical sites. American Institute of Chemical Engineers: New York. ISBN 978-0-470-92500-3.
- Gerbec, Marko, Giunta, Gabriele. InfraStress approach on risk modelling of cascading events with live data for decision support. In: Soldatos, John (Ed.), Praça, Isabel (Ed.), Jovanović, Aleksandar (Ed.). Cyber-physical threat intelligence for critical infrastructures security : securing critical infrastructures in air transport, water, gas, healthcare, finance and industry, (NowOpen). Hanover: Now Publishers. 2021, 2-21, DOI: 10.1561/9781680838237.
- Uijt de Haag P.A.M., Ale B.J.M., 2005. Guideline for quantitative risk assessment 'Purple book', CPR 18E. http://content.publicatiereeksgevaarlijkestoffen.nl/documents/PGS3/PGS3-1999-v0.1-quantitative-risk-assessment.pdf
- Suarez-Paba Maria Camila, Perreur Mathis, Munoz Felipe, Cruz Ana Mariad, 2019. Sys-tematic literature review and qualitative meta-analysis of Natech research in the past four decades. Safety Science, 116, 58–77.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

ATLANTIS

References used

- Krausmann Elisabeth, Cruz Ana Maria, Salzano Ernesto, (Eds), 2017. Natech Risk As-sessment and Management Reducing the Risk of Natural-Hazard Impact on Hazardous Installations. Elsevier. ISBN: 978-0-12-803807-9.
- EC, JRC, Institute for the Protection and Security of the Citizen, 2008. Understanding Malicious Attacks against Infrastructures - Overview on the Assessment and Manage-ment of Threats and Attacks to Industrial Control Systems. Bogdan Vamanu, Marcelo Masera. EUR 23681 EN. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC49474/understanding%20malicious%20attacks%20against%20infrastructures.pdf.
- ENISA report on threats in the area of smart grids and good practice guide. 17.12.2013. https://www.enisa.europa.eu/sites/default/files/publications/Smart%20Grid%20Threat%20Lanscape.pdf
- Camino Kavanagh, 2019. New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses? Carnegie Endowment for International Peace. https://carnegieendowment.org/files/WP_Camino_Kavanagh____New_Tech_New_Threats1.pdf
- Chapter 4: FDI and National Security: Separating Legitimate Threats from Implausible Apprehensions. In: Foreign direct investment in the United States: Benefits, Suspicions, and Risks with Special Attention to FDI from China, 3RD EDITION, Edward M. Graham (PIIE) and Paul R. Krugman, January 1995. ISBN: 978-0-88132-204-0.
- REGULATION (EU) 2019/452 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union; https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0452&from=EN.
- European Commission, Study on the EU’s list of Critical Raw Materials – Final Report (2020). ISBN 978-92-76-21049-8, doi: 10.2873/11619.

This project has received funding from the European Union’s Horizon Europe research and innovation programme under the grant agreement No 101073878.

Questions?

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.