

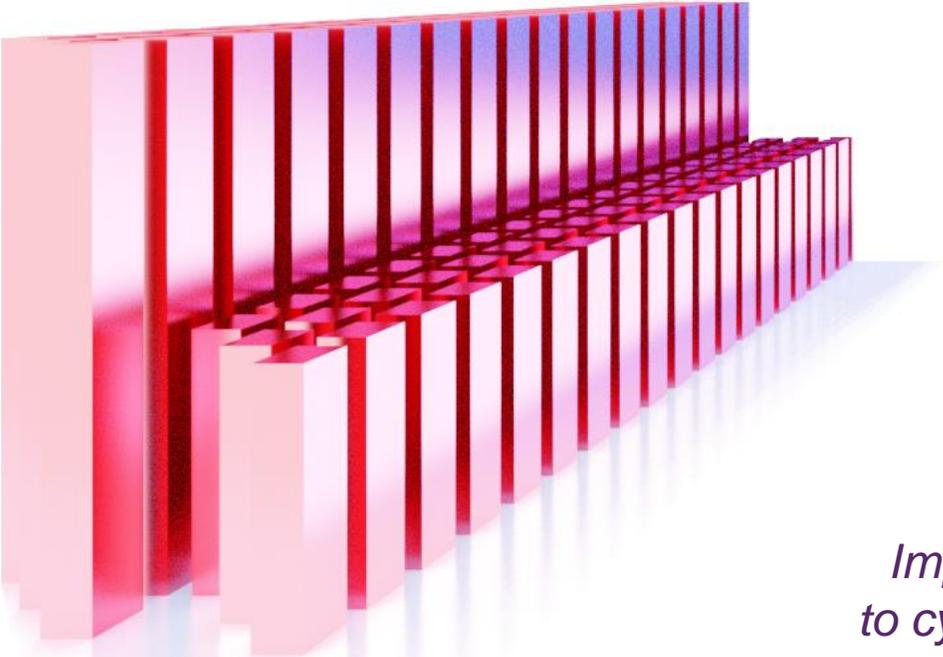
INFRASTRESS PROJECT

PROTECTING THE INFRASTRUCTURE OF EUROPE AND THE PEOPLE IN THE EUROPEAN SMART CITIES

A. Jovanovic, L. Sutton

InfraStress Scientific Manager
&
InfraStress Project Coordinator

Shaping the future of cybersecurity - Priorities, challenges
and funding opportunities for a more resilient Europe
13 July 2021



INFRA STRESS

*Improving resilience of sensitive industrial plants & infrastructures exposed
to cyber-physical threats by means of an open testbed stress-testing system*

MAIN MESSAGE

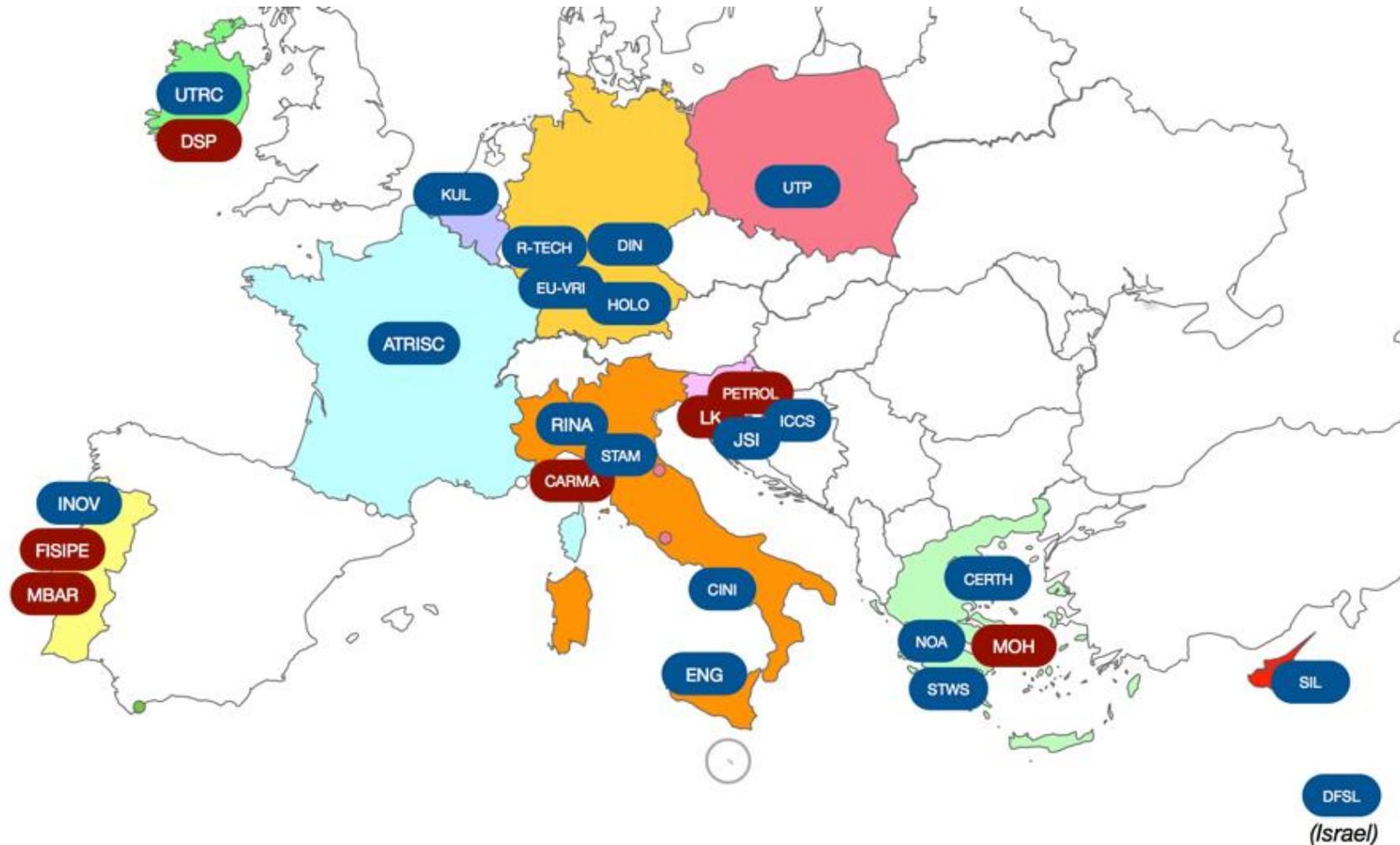


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

INFRA STRESS

InfraStress 2019-2021

- InfraStress brings together 27 partners of excellence from 11 countries
- Cyprus
- France
- Germany
- Greece
- Ireland
- Israel
- Italy
- Netherlands
- Poland
- Portugal
- Slovenia



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

INFRA STRESS



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

INFRA STRESS

InfraStress main objectives

- **Improve the resilience** and the protection capabilities of **Sensitive Industrial Plants and Sites (SIPS)** exposed to large-scale, combined, **cyber-physical threats and hazards**
- **Stress-testing resilience:** Guarantee continuity of **operations**, while minimizing cascading effects in the infrastructure itself, the environment, other Critical Infrastructures (CIs), and the citizens in vicinity, at reasonable cost
- InfraStress deals with **security** of both sensitive industrial production plants and sensitive storage sites, along with ICT infrastructures supporting them



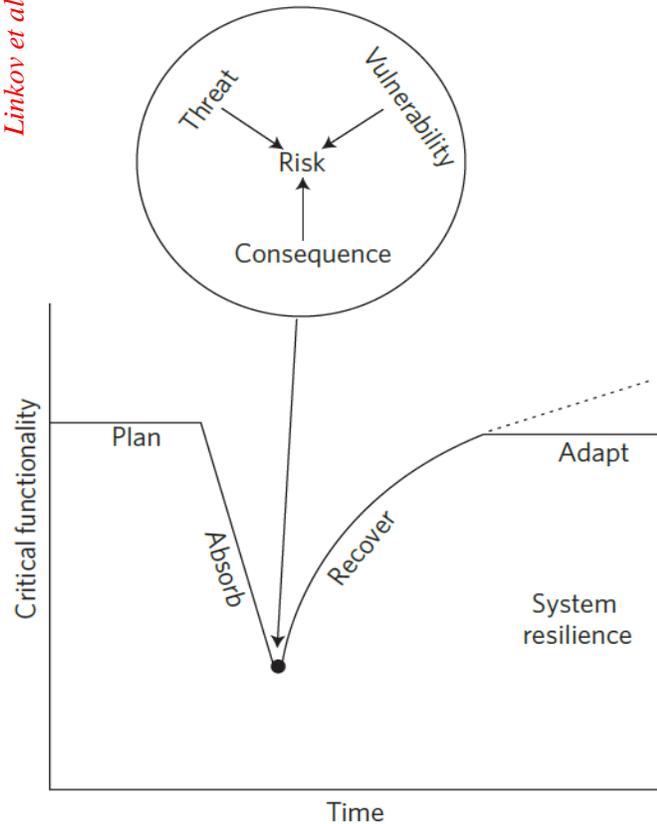
Methodology and expected outcomes

- The **InfraStress methodology** is based on a set of composite indicators of SIPS security and resilience, which will be embedded into the new risk and resilience ISO and CEN standards, and into education and training programs
- The **methodology** and **indicators** will yield breakthrough innovation and the benefits/savings to be achieved by the project will be assessed by users and advisory groups
- **Integrate**
 - Risk & resilience,
 - Safety & security
 - Situational Awareness & resilience

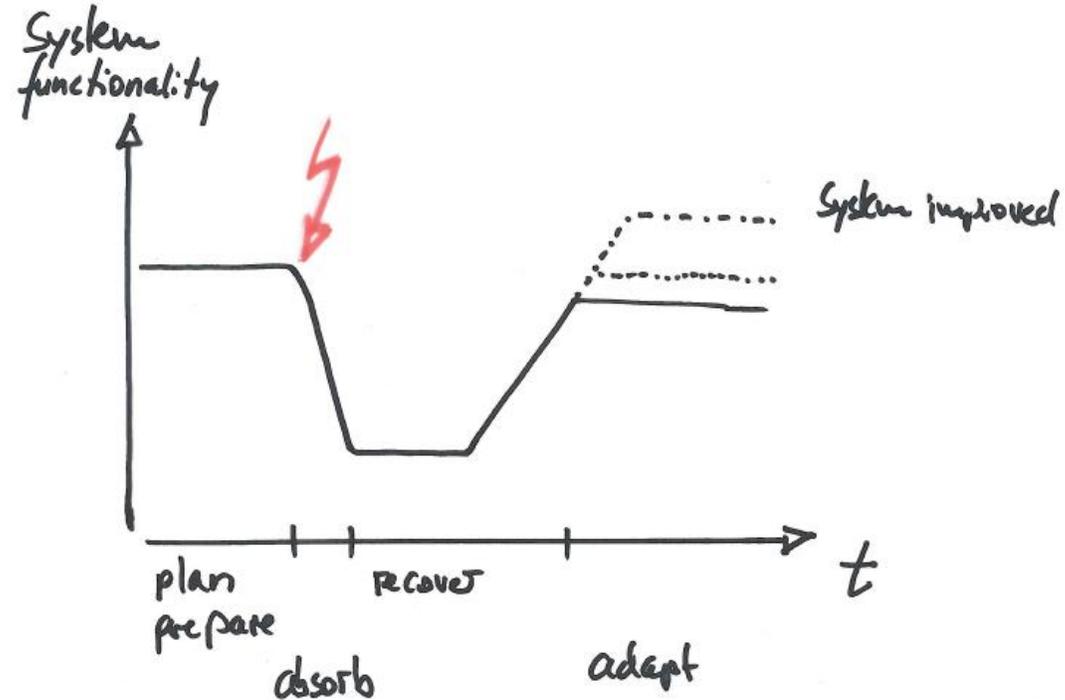


Resilience: what happens when risk happens?

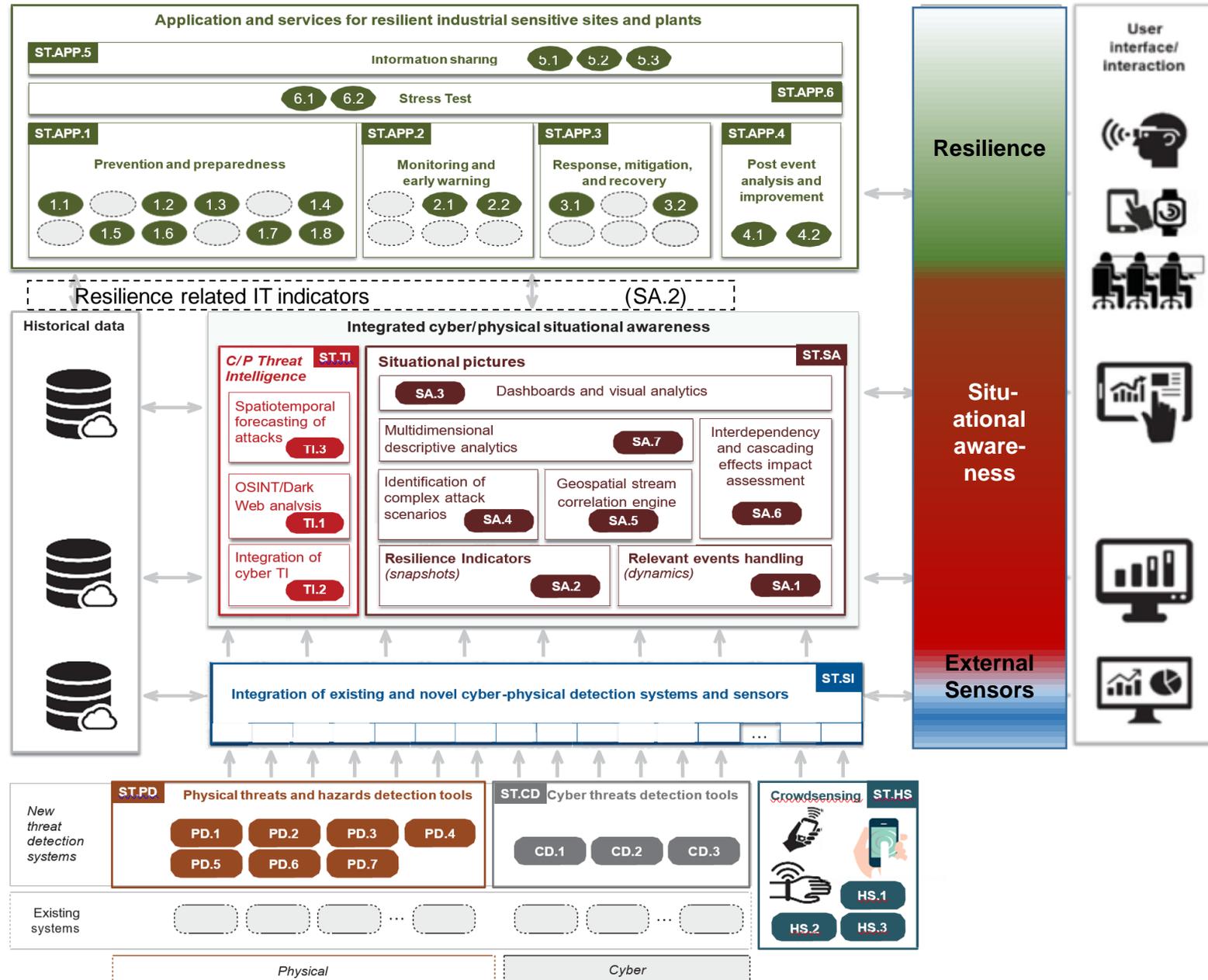
Linkov et al. 2014



- ISO 22300:2018
... ability to absorb and adapt in a changing environment.

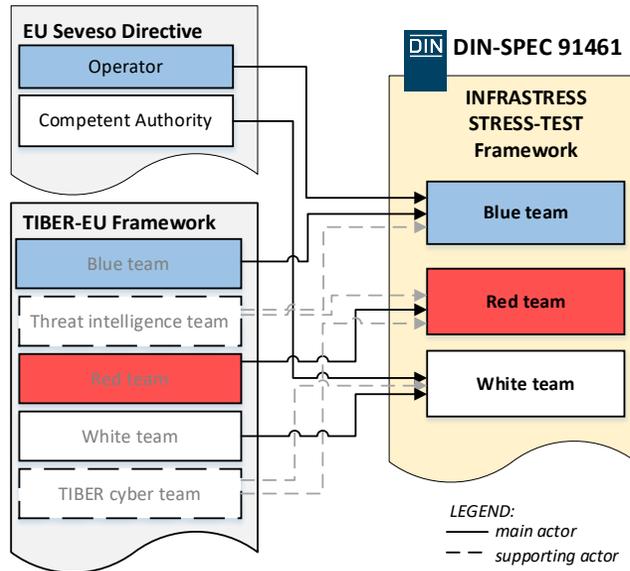


Integration,
Integration,
Integration,
Integration,

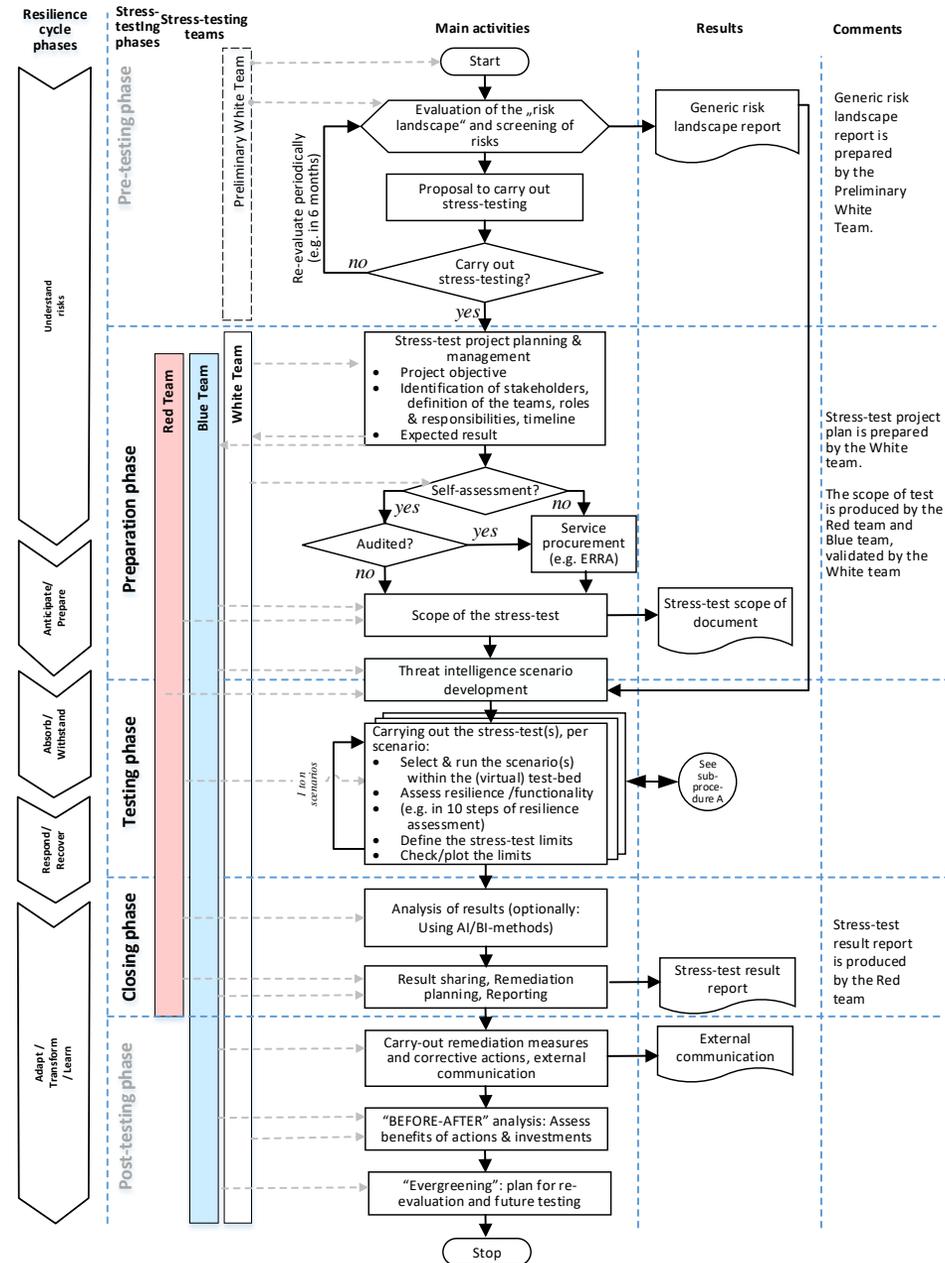


Conclusions: The way forward

- Standardized stress-testing



DIN-SPEC 91461 Resilience Stress-testing Workflow



SUPPORTING DETAILS...



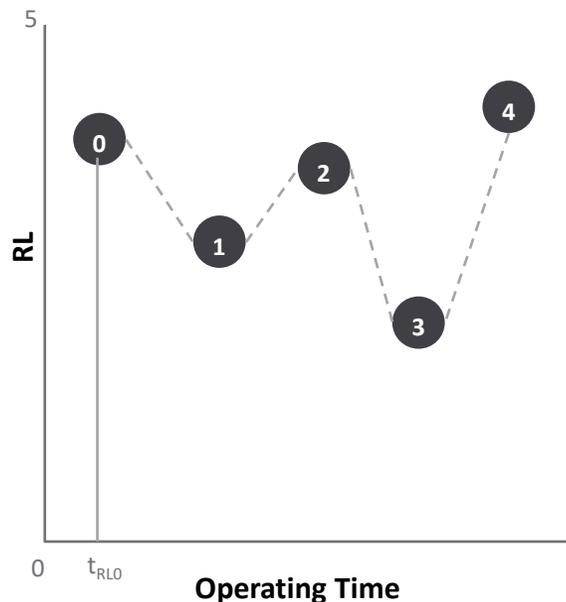
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

INFRA STRESS

Goal

- assess and monitor the **Resilience** of my IT (cyber-physical) infrastructure
- assess the **Functionality** (operational loss) of my infrastructure for a threat/event

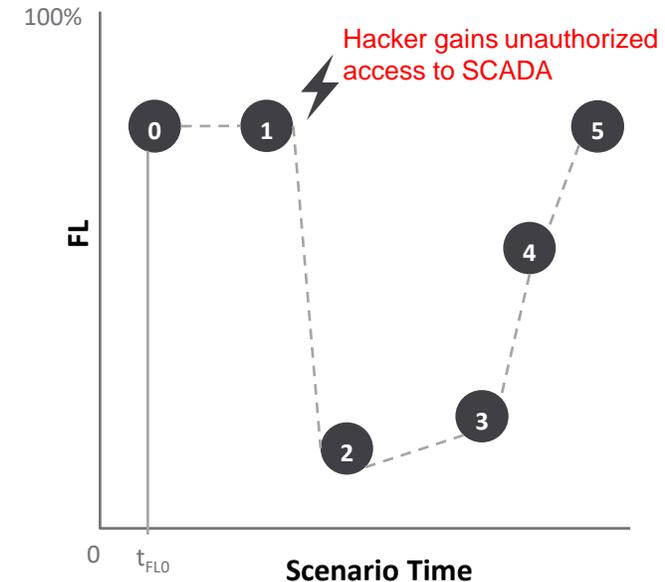
Resilience level (RL) Assessment



Assessment

- 0 Time t_0
- 1 Time t_1
- 2 Time t_2
- 3 Time t_3
- 4 Time t_4
- ⋮
- n Time t_n

Functionality level (FL) Assessment

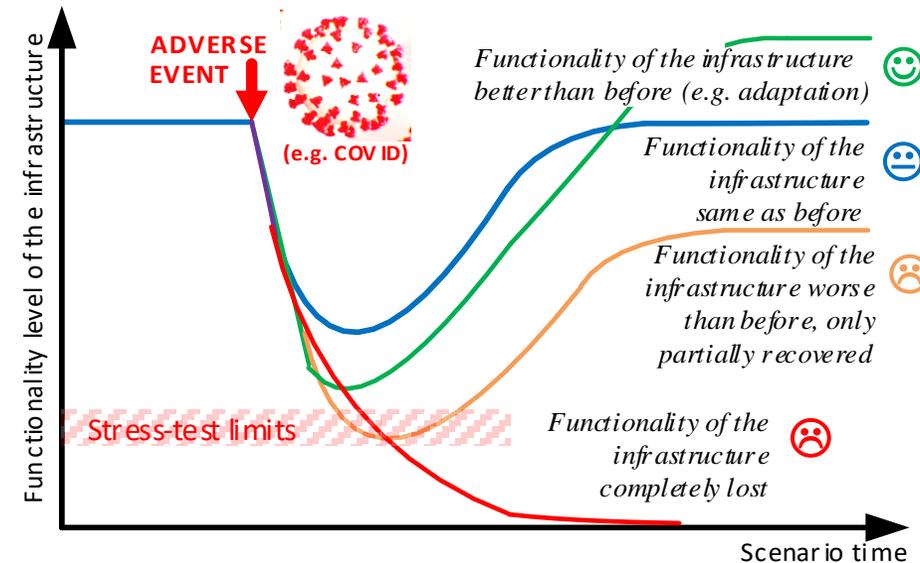
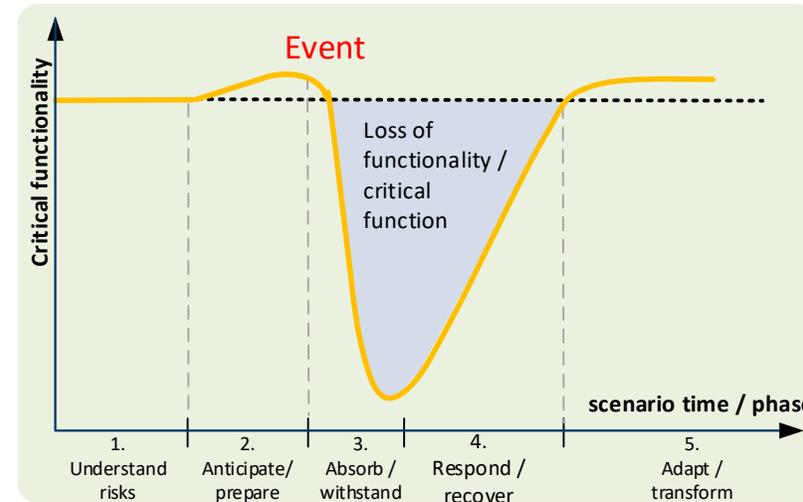


Resilience: what happens when risk happens?

SmartResilience project – “smart critical infrastructures”:

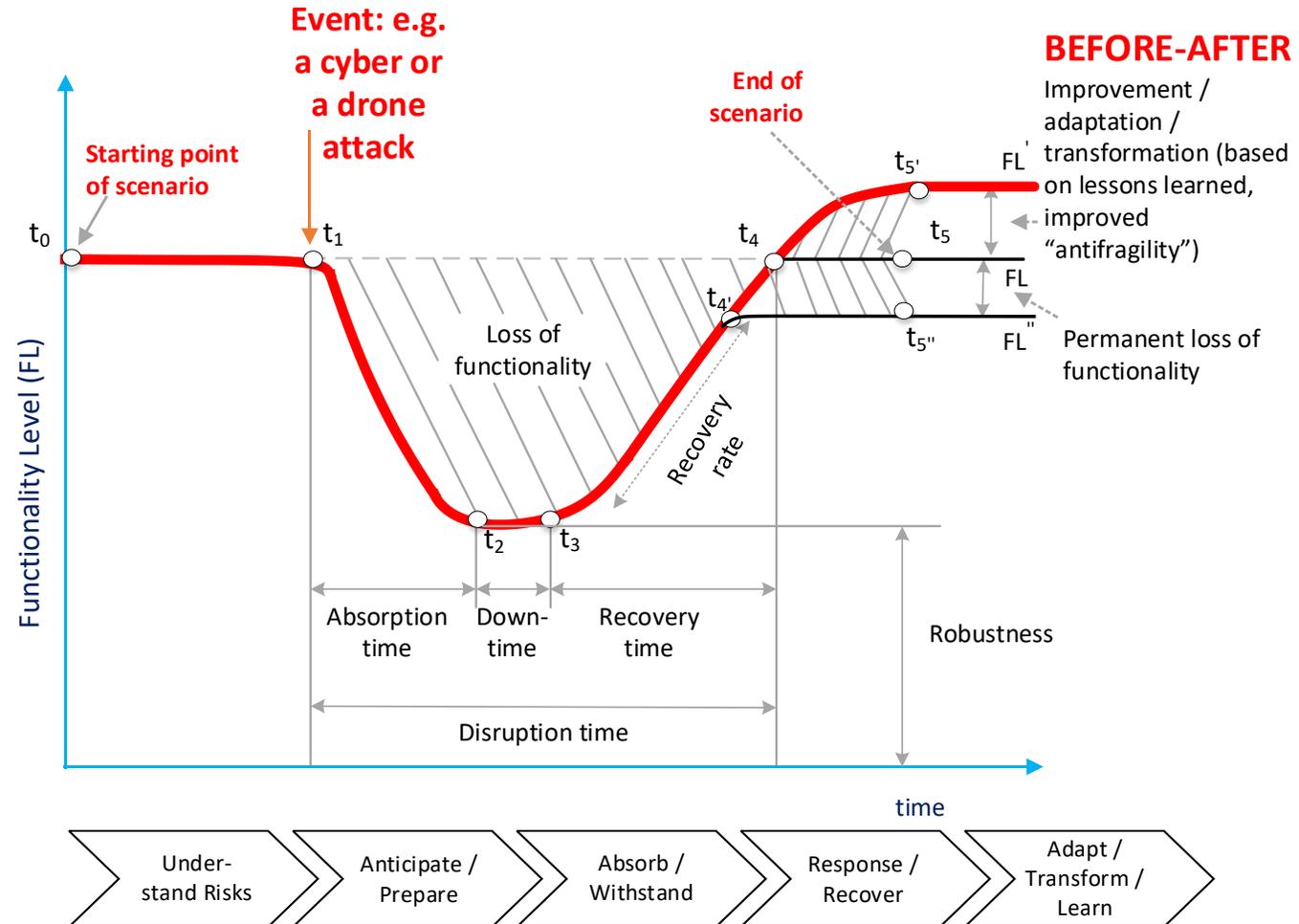
... ability to

- 1. understand and anticipate risks** – including new/emerging risks – threatening the critical functionality of the infrastructure,
- 2. prepare** for anticipated or unexpected disruptive events, optimally
- 3. absorb/withstand** their impacts,
- 4. respond and recover** from them, and
- 5. adapt/transform** the infrastructure or its operation based on lessons learned, thus reducing the critical infrastructure fragility.

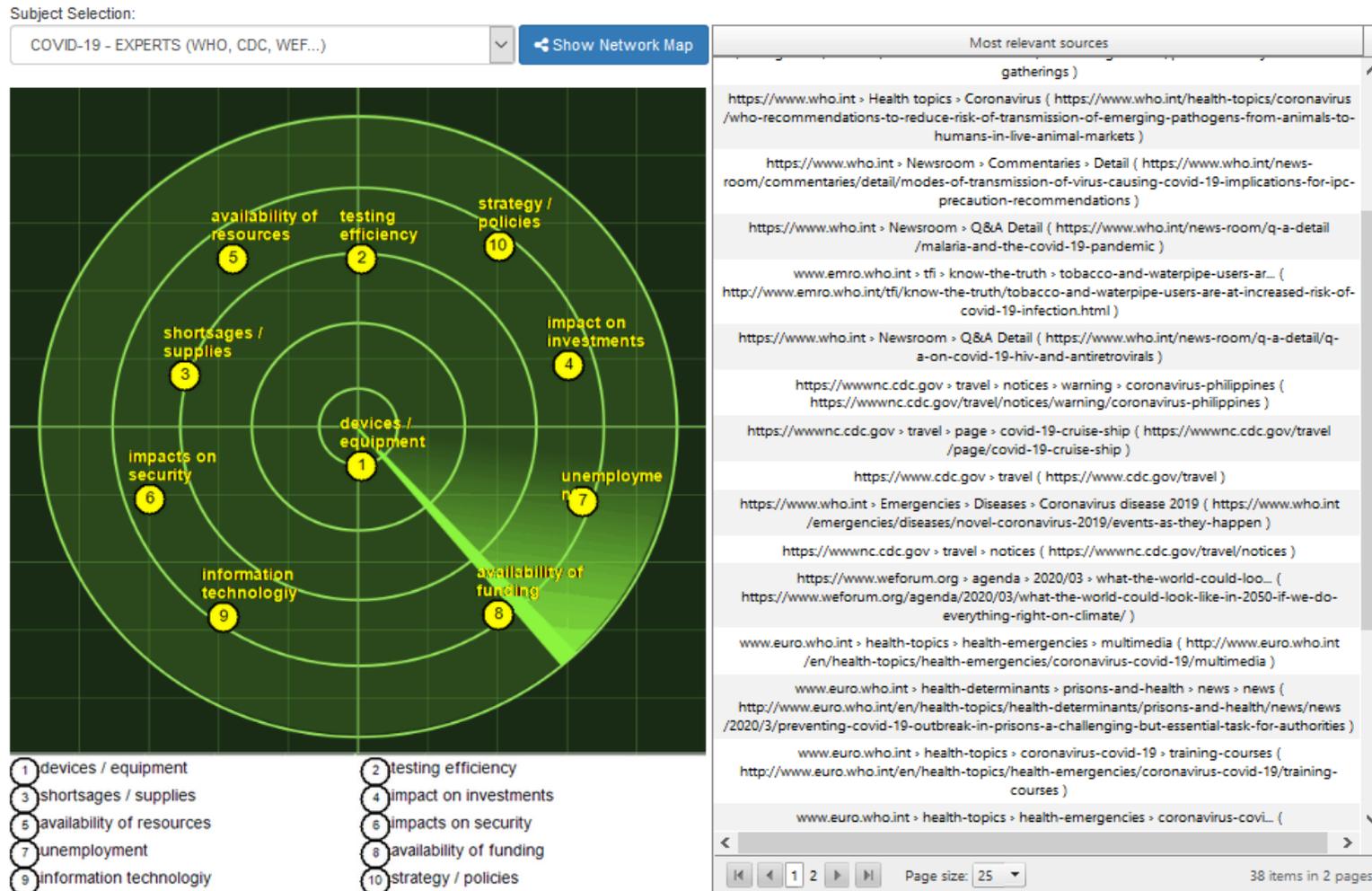


Integration of tasks and deliverables in InfraStress?

Is it not the standard? ERRA?

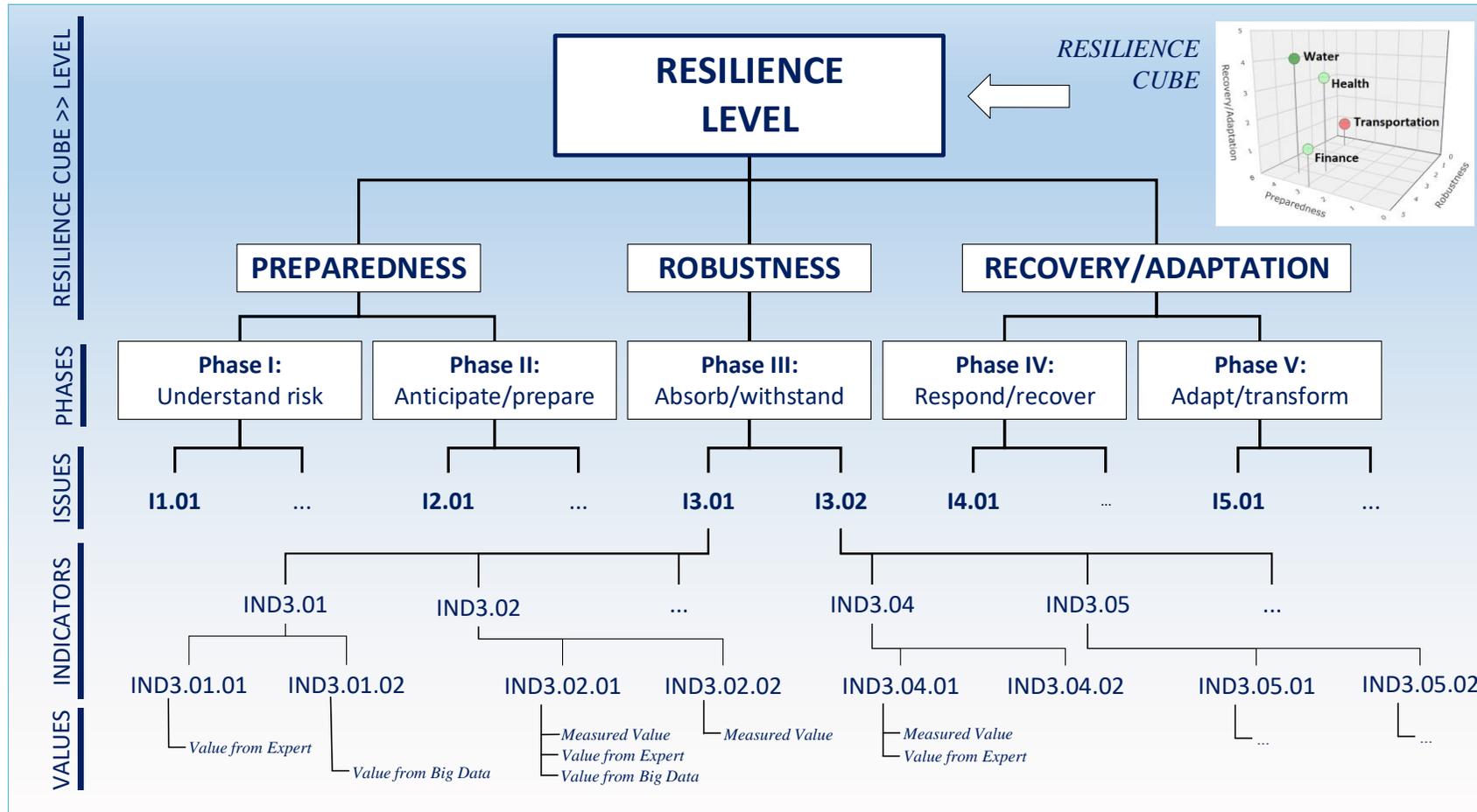


Perceiving threats – emerging risks radar



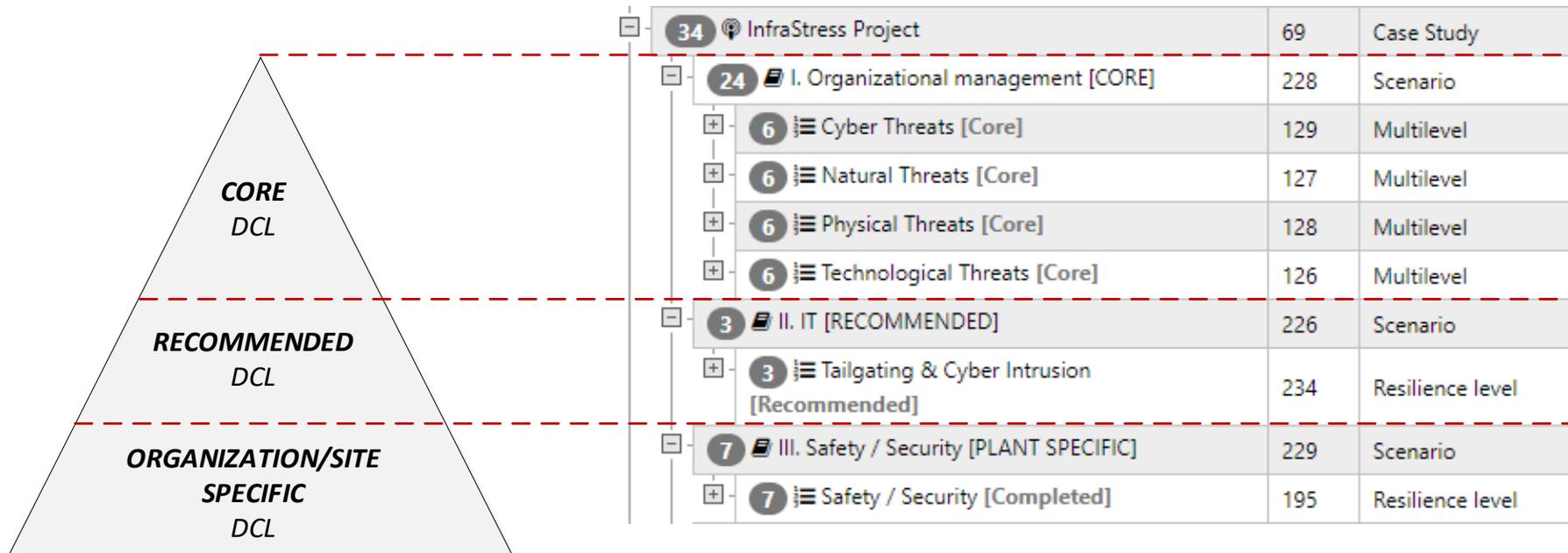
Resilience Level (RL)

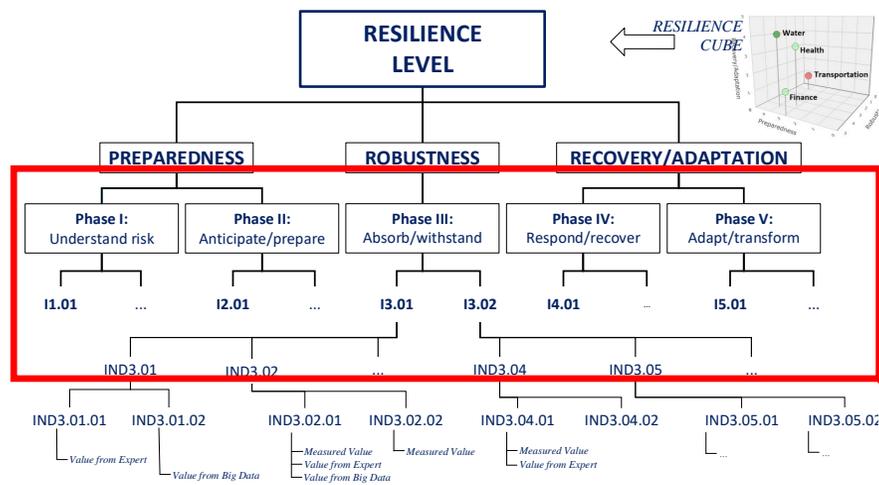
A composite index based on resilience indicators



“Pyramid” of resilience assessment levels

- Crucial for
 - » Understanding of the concept
 - » Use of the





Dynamic Checklist - Setup

IS Pilots Plant wide RL DCL

Step 1: Basic Informa...
Step 2: Issues
Step 3: Indicators
Step 4: Preview

Previous Next

- I. UNDERSTAND RISKS
- II. ANTICIPATE/PREPARE
- III. ABSORB/WITHSTAND
- IV. RESPOND/RECOVER
- V. ADAPT/TRANSFORM
 - Incident investigation; ID-1004
 - Is there an incident investigation and reporting procedure in place?; ID-605
 - Incident related communication exchanged with other relevant sites?; ID-1010
 - Emergency response reporting including lessons learned ; ID-3826
 - Quality of the lessons learned process?; ID-3101
 - Review of lessons learned conducted?; ID-929
 - Does the Company take into account corrective actions in the management of non-compliance?;
 - InfraStress BAM Aware IDS; ID-5674
 - Are the base processes updated in BAM/BPM mapping post event?; ID-5690
 - Are business processes audited on a regular basis post events?; ID-5691
 - SIPS specific corrective action control; ID-5692
 - Is there a closed loop corrective action (CLCA) procedure in the SIP?; ID-5693
 - How frequently do the same root causes appear in incident reports?; ID-3851
 - Post event analysis and procedures to increase resilience; ID-5694

Working with pilot partners, SIPS relevant indicator lists are being developed in preparation for WP8 and implemented in the InfraStress ResilienceTool.

The goal is a single DCL for all participating pilots for standardization and benchmarking.

Integration of tasks and deliverables in InfraStress? Is it not the standard? ERRA?

- **BEFORE-AFTER? What is the quantified impact?**
- **SUGGESTION:** At the end of the pilots
 - » Identify SA-indicators and create the respective DCLs
 - » Assess the “BEFORE” resilience based on the DCLs
 - » Assess the “AFTER” resilience based on the DCLs
 - » Show the improvement based on indicators
 - » Propose



“BEFORE” and “AFTER” resilience assessments at Pilot 4

BEFORE

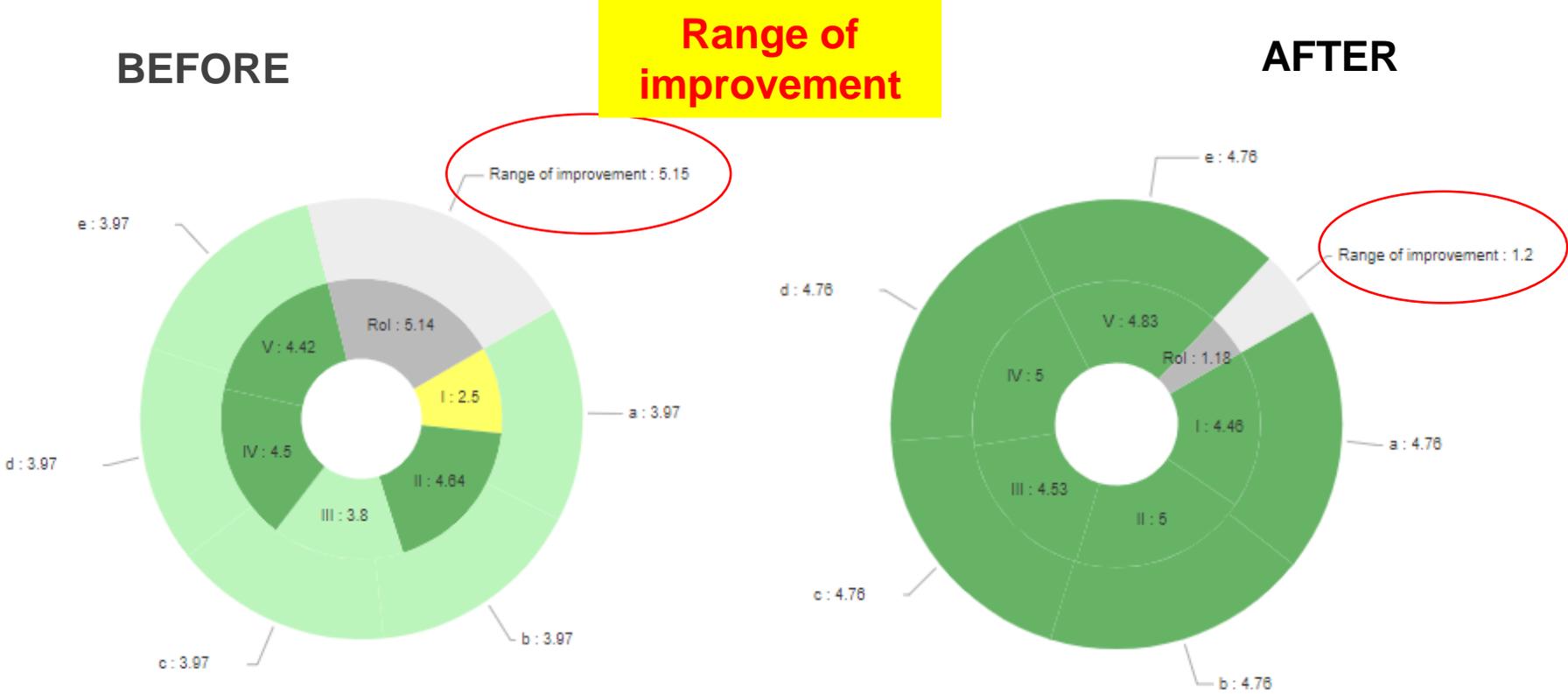
Indicators

AFTER

Name	Type	Syst a	Info b	Org c	Soc d	DeM e	Score	Resilience Level	Name	Type	Syst a	Info b	Org c	Soc d	DeM e	Score	Resilience Level
Resilience index level	Root						3.95	Good	Resilience index level	Root						4.8	Excellent
I.Understand risks	Phase						2.45	Average	I.Understand risks	Phase						4.56	Excellent
I.1. Available formal management systems adopted in the organization; ID-5652	Issue	✓	✓	✓	✓	✓	3	Average	I.1. Available formal management systems adopted in the organization; ID-5652	Issue	✓	✓	✓	✓	✓	4.5	Excellent
I.1.1. Does the organisation hold a ISO 9000 series certification or similar?: ID-5653	Indicator						5	Excellent	I.1.1. Does the organisation hold a ISO 9000 series certification or similar?: ID-5653	Indicator						5	Excellent
I.1.2. Are internal audits and management reviews conducted regularly?: ID-5654	Indicator						5	Excellent	I.1.2. Are internal audits and management reviews conducted regularly?: ID-5654	Indicator						5	Excellent
I.1.3. Is there a formal environmental management system adopted in the organization (e.g., ISO 14000 series or EMAS scheme)? ID-5842	Indicator						5	Excellent	I.1.3. Is there a formal environmental management system adopted in the organization (e.g., ISO 14000 series or EMAS scheme)? ID-5842	Indicator						5	Excellent
I.1.4. Does the organisation hold a valid ISO 14000 series/EMAS certification or similar?: ID-5843	Indicator						5	Excellent	I.1.4. Does the organisation hold a valid ISO 14000 series/EMAS certification or similar?: ID-5843	Indicator						5	Excellent
I.1.5. Is there a formal occupational health as safety management system adopted in the organization (e.g., OHSAS 18001 or ISO 45001 standards)? ID-5844	Indicator						5	Excellent	I.1.5. Is there a formal occupational health as safety management system adopted in the organization (e.g., OHSAS 18001 or ISO 45001 standards)? ID-5844	Indicator						5	Excellent
I.1.6. Does the organisation hold a valid ISO 45001 or OHSAS 8001 certification or similar?: ID-5845	Indicator						0	Critical	I.1.6. Does the organisation hold a valid ISO 45001 or OHSAS 8001 certification or similar?: ID-5845	Indicator						0	Critical
I.1.7. Is there a formal Safety Management System adopted in the organization (aspect of major accidents prevention)? ID-5846	Indicator						0	Critical	I.1.7. Is there a formal Safety Management System adopted in the organization (aspect of major accidents prevention)? ID-5846	Indicator						5	Excellent
I.1.8. Does the organization hold a valid environmental permit for its operations as specific SIPS?: ID-5847	Indicator						0	Critical	I.1.8. Does the organization hold a valid environmental permit for its operations as specific SIPS?: ID-5847	Indicator						5	Excellent
I.1.9. Did the organization implement any related industry sector specific standard/recommendations in its management system?: ID-5848	Indicator						0	Critical	I.1.9. Did the organization implement any related industry sector specific standard/recommendations in its management system?: ID-5848	Indicator						5	Excellent
I.1.10. Does the organization hold a valid certificate related to the possible above mentioned standards/codes?: ID-5849	Indicator						5	Excellent	I.1.10. Does the organization hold a valid certificate related to the possible above mentioned standards/codes?: ID-5849	Indicator						5	Excellent



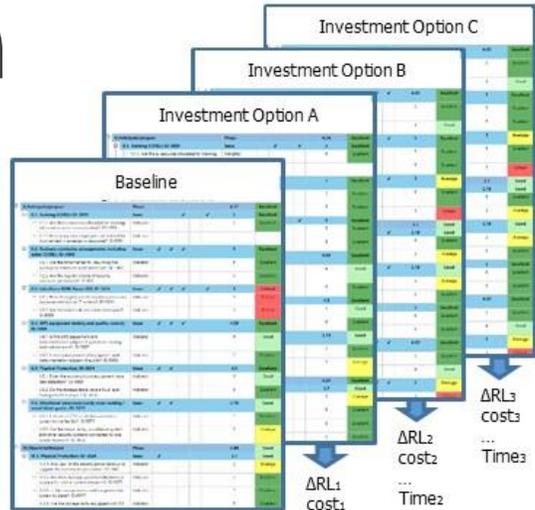
“BEFORE” and “AFTER” resilience assessments at Pilot 4



How to get the best return on investment in resilience?

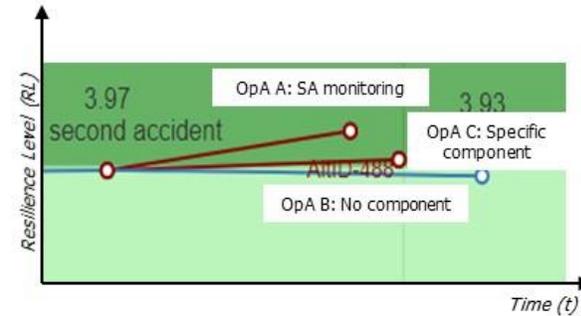
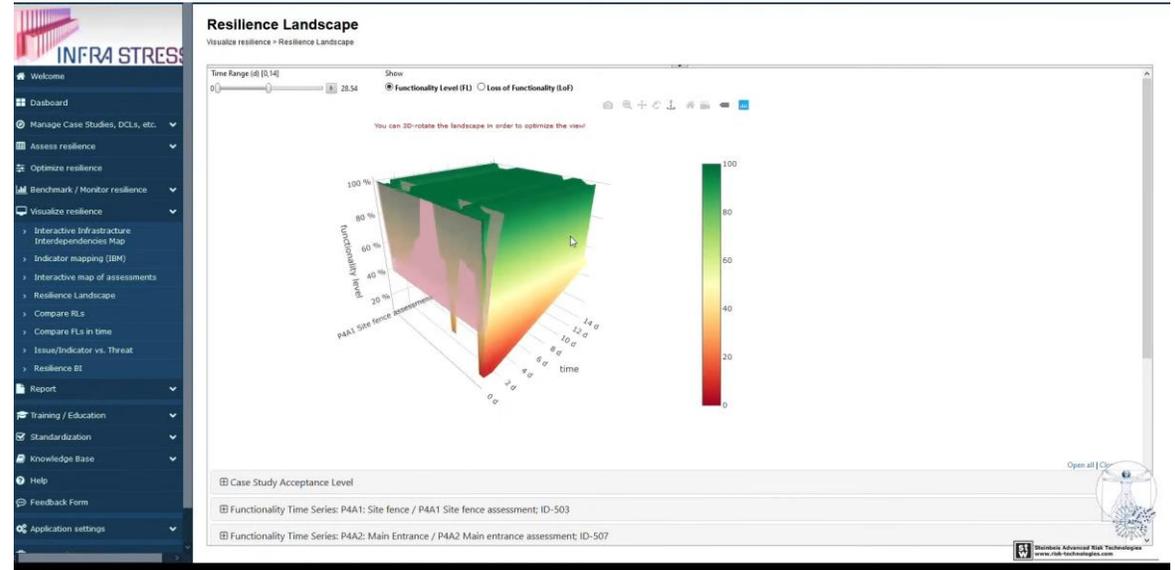
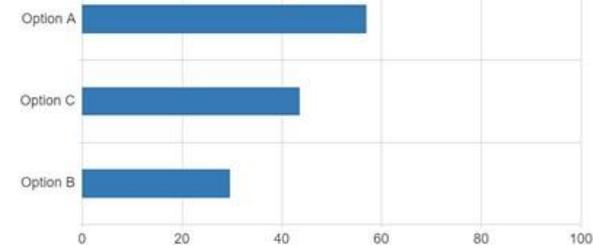
Investment in resilience optimization

Future operation time

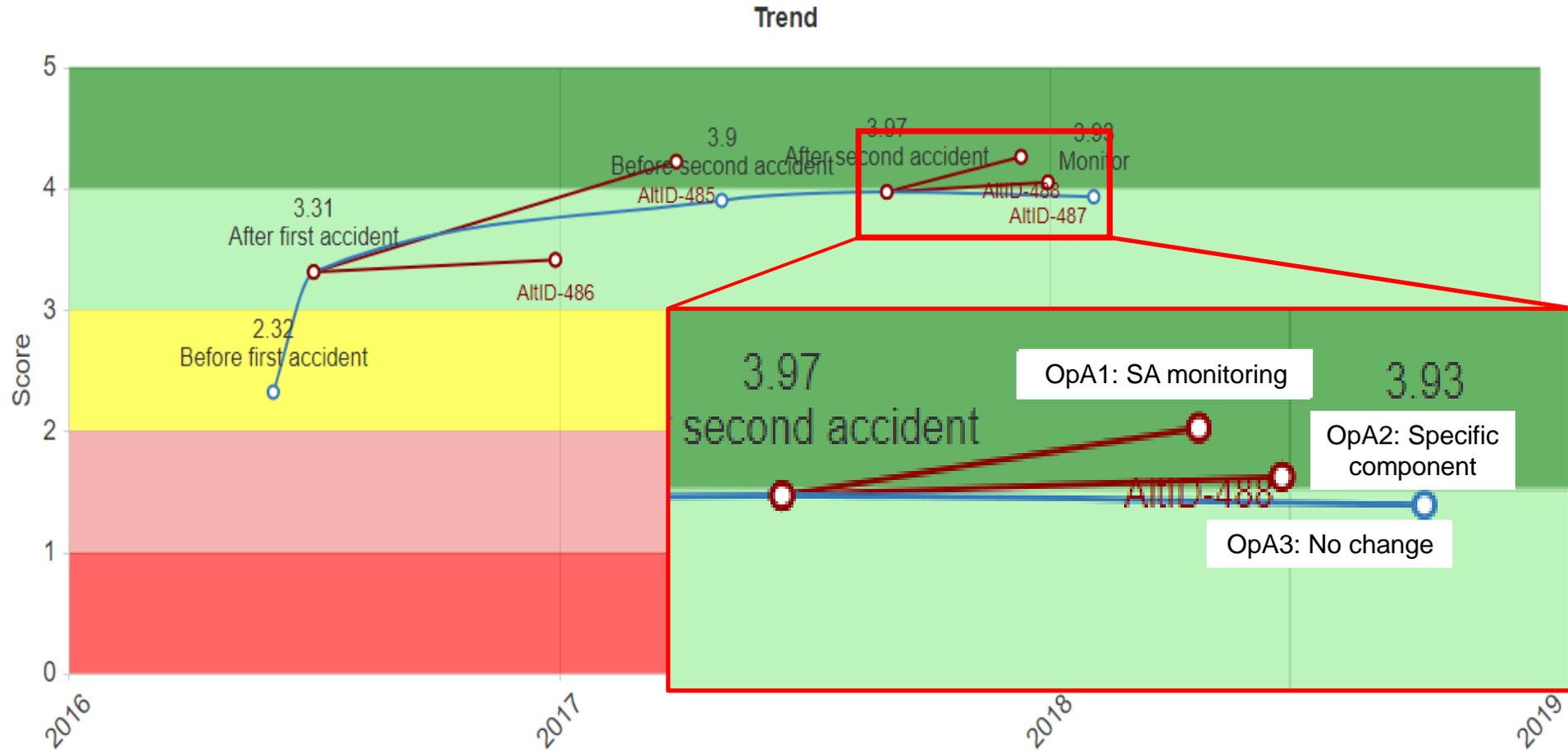


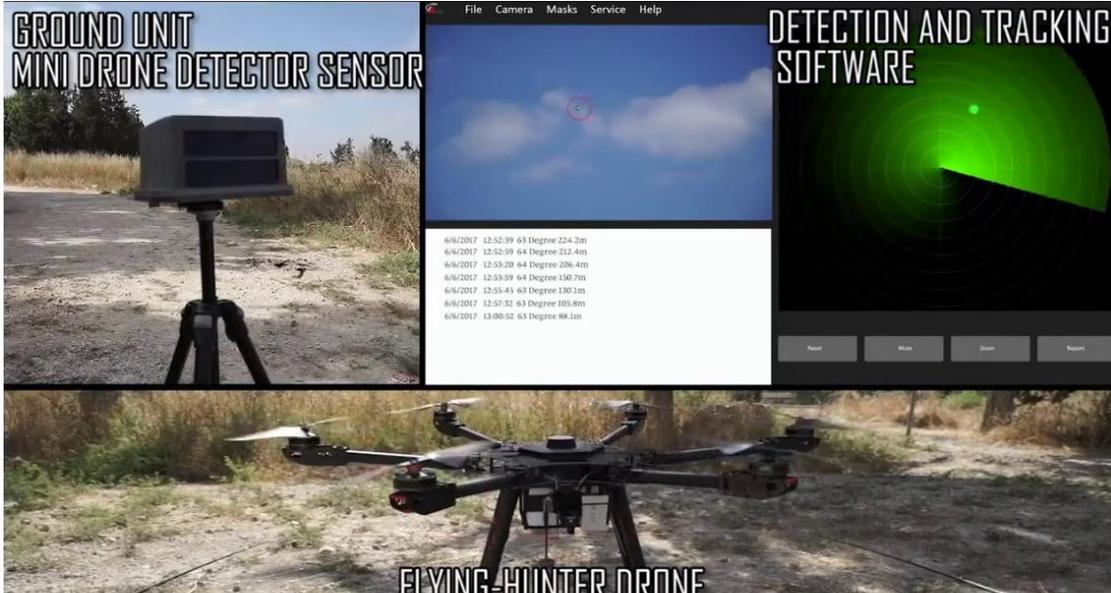
Investment in SA

Option	ΔRL	Total cost	Time	...	Score
A	0.41	\$\$\$	ΣΣ		58.8
B	0.15	\$	Σ		28.1
C	0.23	\$\$	ΣΣΣ		43.7

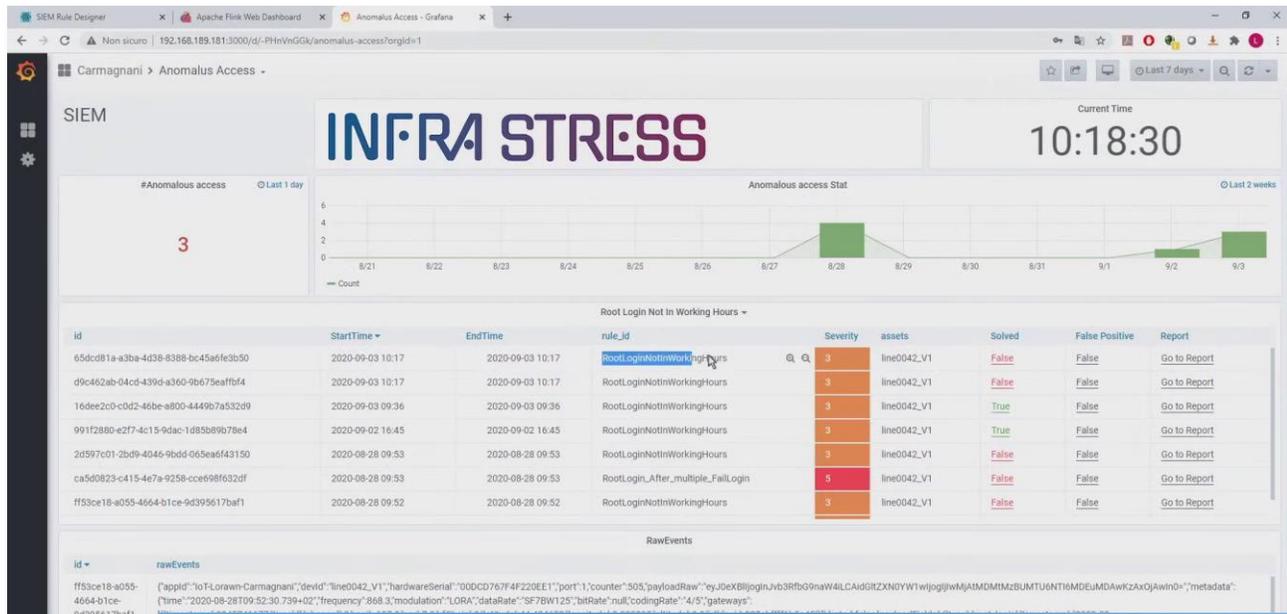


Optimization development in the MCDM tool





Date	Time	Altitude	Distance
6/6/2017	12:52:39	63 Degree	224.2m
6/6/2017	12:52:59	64 Degree	212.4m
6/6/2017	12:53:20	64 Degree	206.4m
6/6/2017	12:53:59	64 Degree	198.7m
6/6/2017	12:54:49	63 Degree	130.1m
6/6/2017	12:57:31	63 Degree	105.8m
6/6/2017	13:00:52	63 Degree	88.1m



SIPS Infrastructure

AREAS: TUNNEL OF MOH CI, WARNING LEVEL 1

ASSETS: 11:29:43, 6/08/2021

MITIGATION ACTIONS:

- 12:40:44, 6/08/2021
- 6/08/2021 - 12:40:44
- 6/08/2021 - 12:40:44
- 6/08/2021 - 12:40:44

MAN DOWN: INFORM THE NATIONAL HEALTH SYSTEM IF HOSPITAL IS NEEDED

SIEM Rule Designer

Nodes: Source, Filter, Count, Join, Enrich, Output

Functions: Render, Clear, Job Manager, Import project

Animations: []

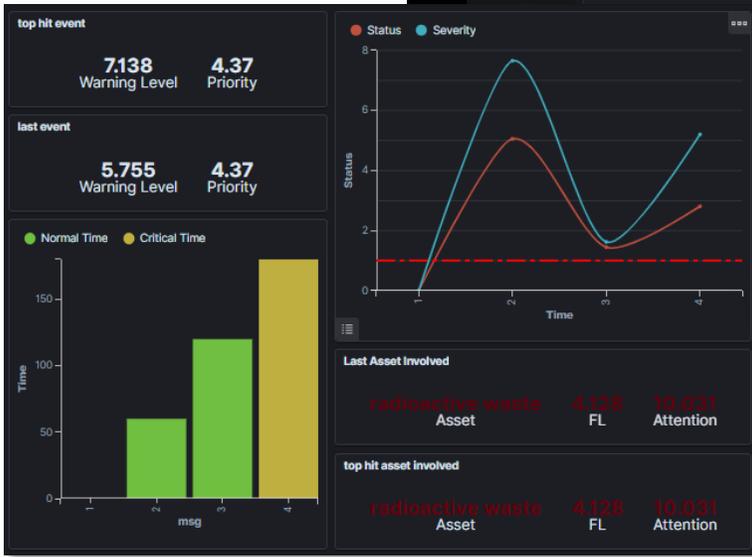
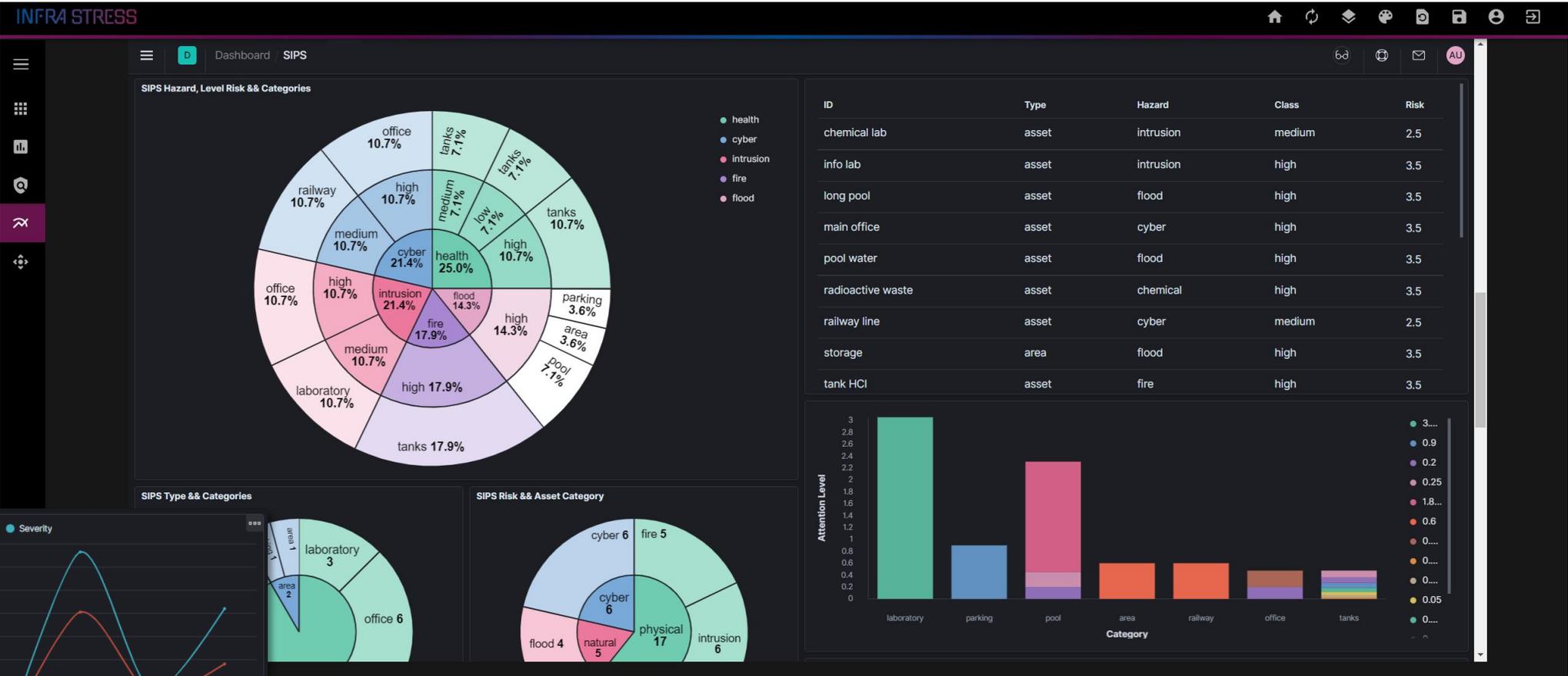
Flowchart: InWorkingHours (In) -> Filter_device (In) -> Count (In) -> Output_6 (In)

BusinessProdMonitoring (Out) -> Filter_Ant (In) -> Count (In) -> Output_6 (In)



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

INFRAS STRESS



SIPS Status

SIPS:	Last Update	Severity	Status	Active/Total events	Assets Involved	Active/Total Actions
MOHQ	🕒	🔋	⚠️	2 / 2	2 / 4	4 / 7



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

[View Other Tools](#)

Risk Assessment Tools

Physical

Natural

Cyber

PHYSICAL

[Learn more](#)

NATURAL

[Learn more](#)

CYBER

[Learn more](#)

Assessments Status

Physical Assessment

Natural Assessment

Cyber Assessment

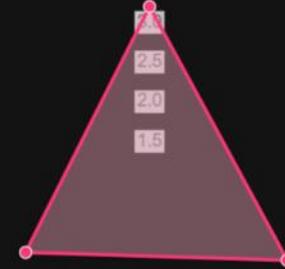
Overall Likelihood Based on a 1 to 5 scale

■ Initial Likelihood
 ■ Contextual Likelihood
 ■ Refined Likelihood

Assessment Area Based on a 1 to 5 scale

Human

- 5.0
- 4.5
- 4.0
- 3.5
- 3.0
- 2.5
- 2.0
- 1.5



MOH

14/6/2021 - 16:00:07

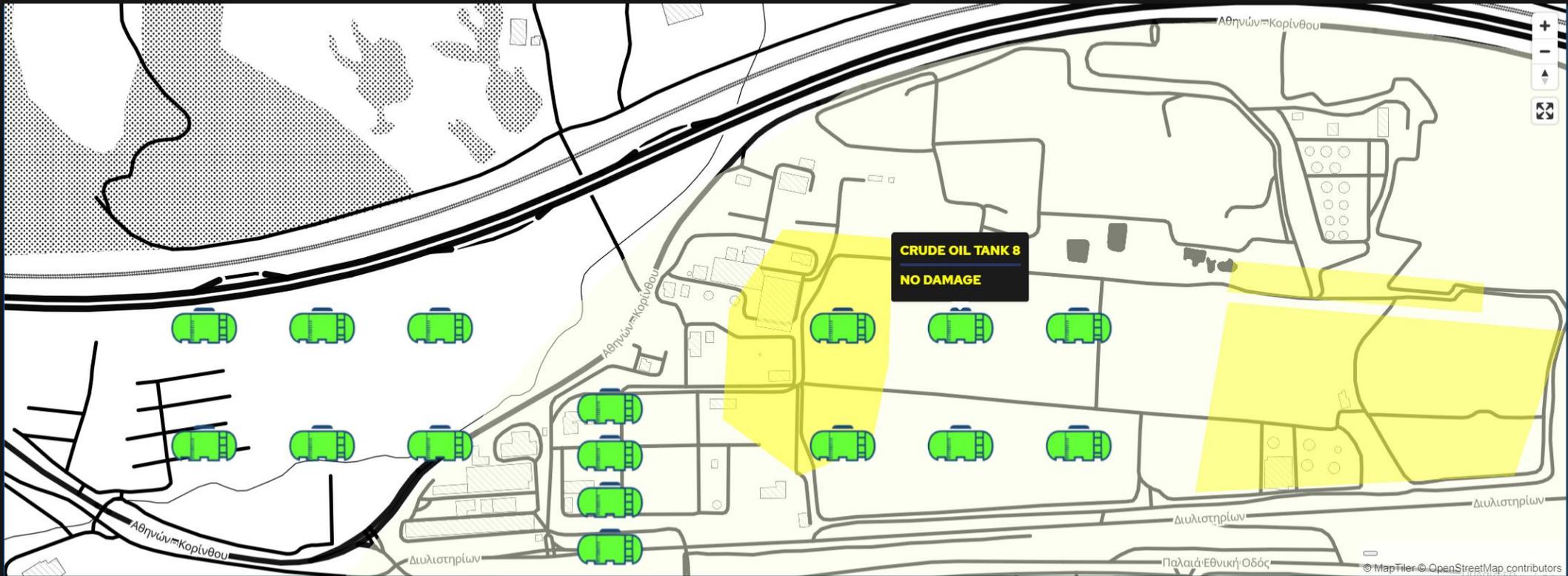
HIGH

CRITICAL

2/2

2/4

5/8



AREAS

ASSETS

<p>MAIN MOH REFINERY AREA</p> <p>WARNING LEVEL:1</p>	<p>17:37:27</p> <p>16/6/2021</p>	<p>📄</p> <p>⌵</p>
<p>MAIN MOH REFINERY MAIN ENTRANCE</p> <p>WARNING LEVEL:1</p>	<p>17:37:27</p> <p>16/6/2021</p>	<p>📄</p> <p>⌵</p>

CURRENT SITUATION

HISTORICAL

<p>📍 +</p>		
<p>COMPLEX ATTACKS</p>	EVENTS	MITIGATION ACTIONS
<p>FORCED ENTRANCE</p>		15:59:18 ⌵



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

InfraStress Pilots

- InfraStress solutions are being tested and demonstrated in **5 SIPS pilots involving the owners/operators** (4 Seveso) as well as their neighbouring facilities from 5 EU Countries (Italy, Portugal, Ireland, Greece, Slovenia): a design-implementation-validation approach.
- Piloting at evaluation and integrating **input from the involved stakeholders** and the feedback from the pilot execution.
- Pilots collectively cover a variety of high-impact **multithreat scenarios** to SIPS CIs, ranging from natural disasters to direct cyber-physical attacks to critical assets
- Last, but not least: The InfraStress solutions will be “anchored” in the new ISO **31050** standard (“**Guidance for managing emerging risks to enhance resilience**”)



Pilot 1: Motor Oil Hellas - Greece



Refinery – Petrolchemicals



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

INFRA STRESS

Pilot 2: DePuy Synthes, Cork - Ireland

Medical manufacturing plant (orthopaedics)



DePuy is a franchise of Johnson & Johnson



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

INFRA STRESS

Pilot 3: Carmagnani, Genoa - Italy



Chemical storage site and terminal



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

INFRA STRESS

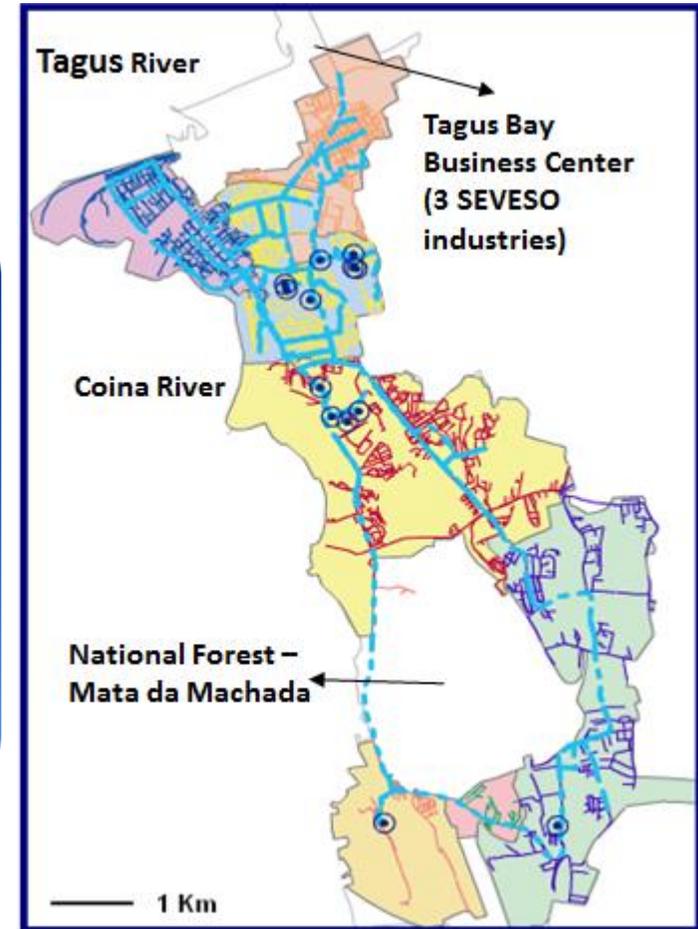
Pilot 4: Petrol + Port of Koper - Slovenia



Petrol infrastructure for storing and transport of fuel and Port of Koper terminal



Pilot 5: Municipality of Barreiro + SGL



SGL industrial facilities and Barreiro municipality critical infrastructure

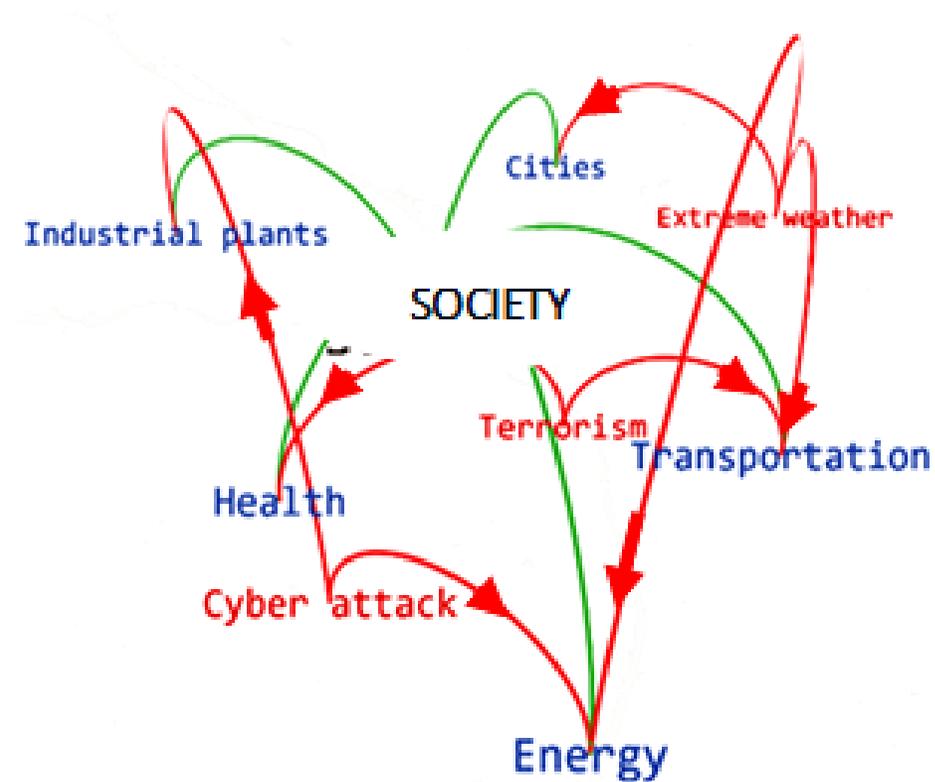


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833088

INFRA STRESS

Conclusions

1. Away from (just) first response
2. Integrate
 - Past (cases, experience..)
 - Present (situational awareness, “radars”)
 - Future (scenario/resilience analysis)
3. Increase resilience & efficiency, decrease vulnerability of the society as infrastructure/network-of-critical-infrastructures/functions
4. Interdependencies
5. x-Threats (multiple/new/unknown/emerging threats)



www.infrastress.eu

info@infrastress.eu



[@InfraStress](https://twitter.com/InfraStress)



[LinkedIn](https://www.linkedin.com/company/InfraStress)



tinyurl.com/infrastress-yt

Aleksandar Jovanovic

jovanovic@risk-technologies.com

Lorenzo Sutton

lorenzo.sutton@eng.it

INFRA STRESS

Improving resilience of sensitive industrial plants & infrastructures exposed to cyber-physical threats by means of an open testbed stress-testing system

