Policies for Resilience of Critical Infrastructure Protection with Dynamic Changes of Operational Conditions: SUNRISE project insights

Aljosa Pasic (ATOS/EVIDEN)

10/12/2024

ATLANTIS, EU-CIP, and ECSCI Cluster Joint Webinar

SUNRISE

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101073821

Outline

SUNRISE

01 SUNRISE project

02 Main Pillars
- Collaboration
- Strategy
- Technology

03 Challenges of Dynamic Conditions
- Observation
- Orientation

04 Policy Task Force
- Methodology
- Results

05 Conclusions

SUNRISE project at a glance

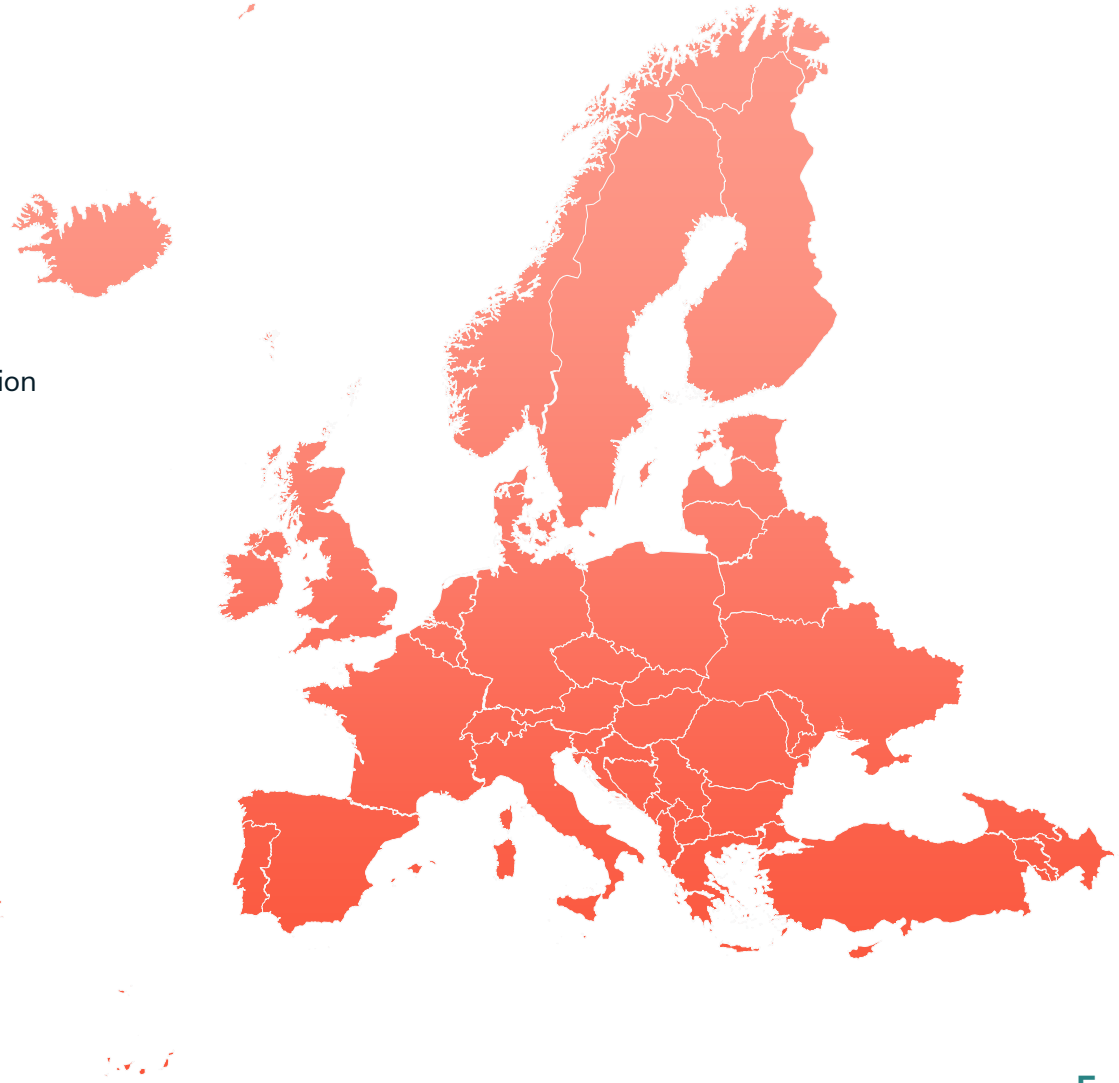
SUNRISE at a glance

Strategies and Technologies for United and Resilient Critical Infrastructures and Vital Services in Pandemic-Stricken Europe	
Call	HORIZON-CL3-2021-INFRA-01
Grant Agreement	101073821
Website	https://sunrise-europe.eu/
Duration	36 Months (01-10/2022 – 30/09/2025)
Budget	Around 11,5 M€
Consortium	42 partners
Project Coordinator	Aljosa Pasic (Atos / Eviden)
Objectives	***O1:*** *Facilitate collaboration among CIs within and across European borders, within and across different sectors, between public and private stakeholders* ***O2:****Identify pandemic-specific vital services and CIs in Europe, their interaction and dependencies, the risks and cascading effects among them, and effective countermeasures at European level* ***O3:*** *Develop a comprehensive strategy and a set of mature technologies for CIs resilience and business continuity in a pandemic* ***O4:****Pilot the new strategy and technologies in real-world conditions across Europe* ***O5:****Enhance knowledge, awareness and capacities for unity and resilience in Europe*

SUNRISE Pilots

SUNRISE

+ **18 pilots in 8 different countries**
  - Most pilots are in ES, IT and SI, defined as strategic national clusters
  - There are some others in FR, EE, RS, IL and CZ
  - Represented sectors: Health, Digital, Energy, Transport, Water and Public Administration
+ **Participation of National Ministries**
  - Internal Affairs in ES
  - Infrastructures in SI
+ **Participation of Regional Government:** Friuli Venezia Giulia in IT
+ **Participation of Municipality:** Jerusalem in IL



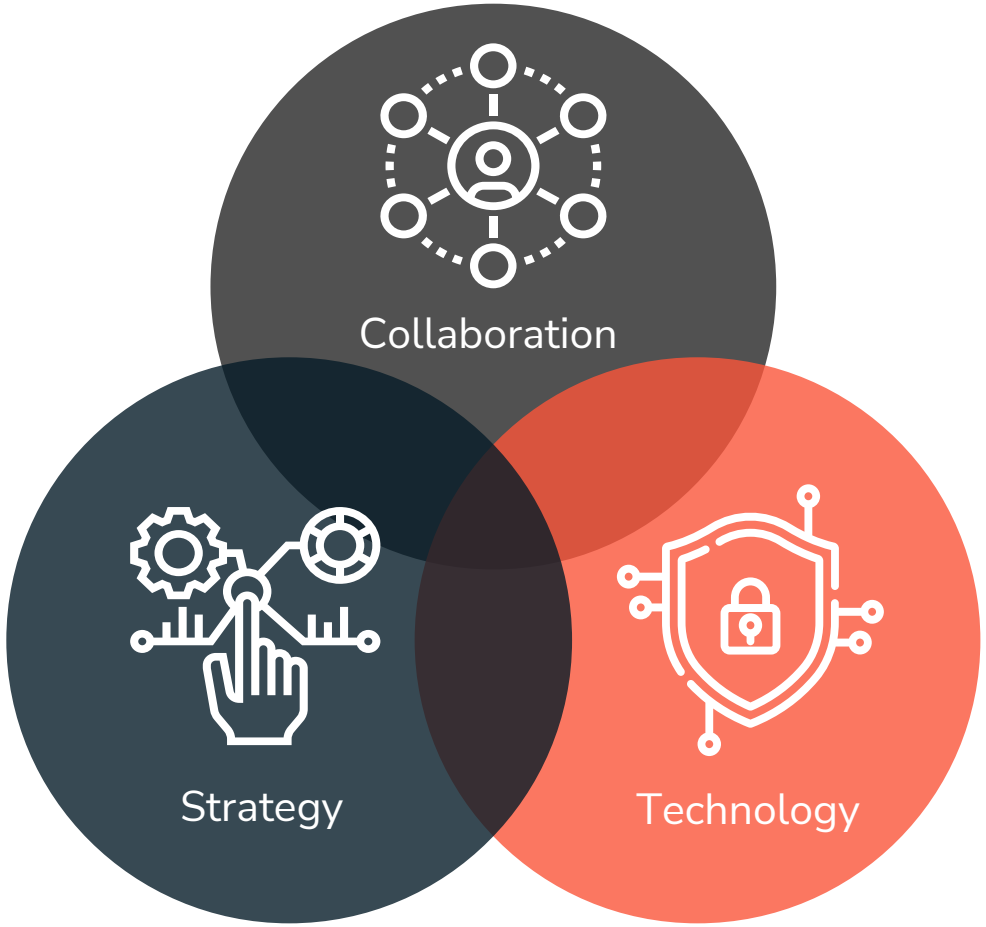
Main Pillars

Mission Statement

SUNRISE

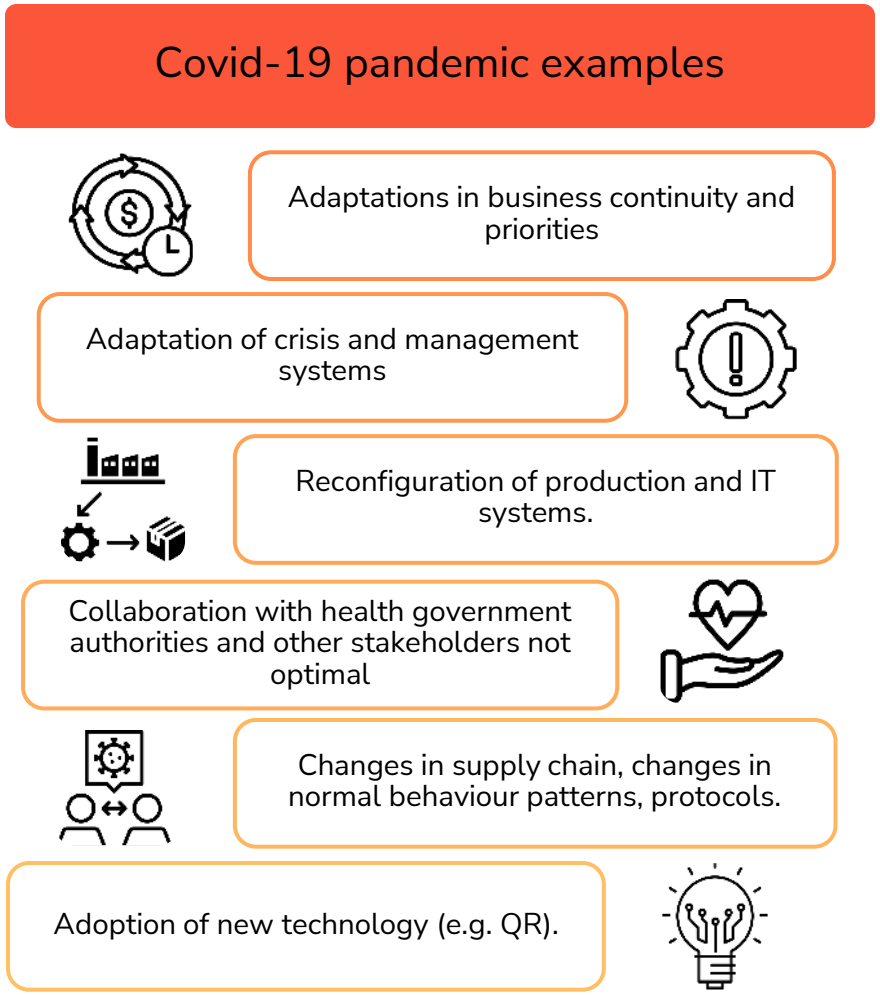
"Strengthening Critical Infrastructures through Collaboration, Strategy and Technology"

- BEFORE: Critical infrastructures' preparedness for emergency scenarios and temporary conditions. Consideration of human factors and climate change as a 'threat multiplier'
- DURING: Adaptable mitigation and collaboration when those scenarios materialize.
- AFTER: Lessons learned, and alignment of strategy and Business continuity plans with uncertain availability of skilled workers and other "temporary condition threat multipliers"



Retro-assessment about IT systems of CI operators

SUNRISE



- **Essential employees** and operators of digital parts of CIs were **affected physically and mentally,** both directly and indirectly, producing increased absenteeism.
- Measures implemented to contain pandemic spread (e.g. lockdown, restrictions) sometimes **destabilized normal maintenance and support** of cyber infrastructure, or incident response teams.
- Changes of national, regional or organizational strategy had an **impact on priority**, as well as the collaboration with the other operators of CIs

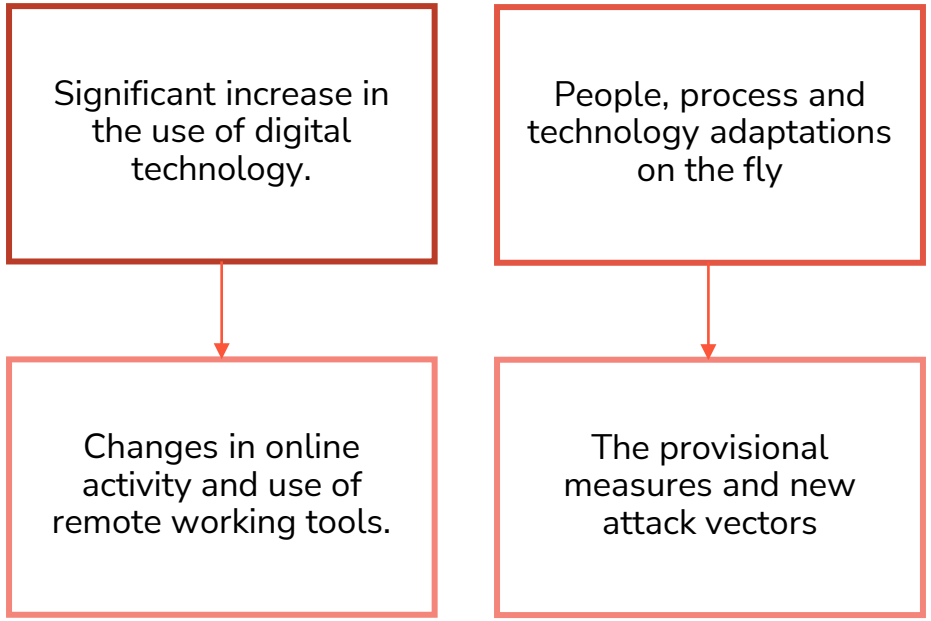
Challenges of Dynamic Operational Conditions

Observation and Orientation

SUNRISE

- OODA loop (Observe, Orient, Decide, Act) focuses on **contextualization** of the available information, while also **making sense** of newly arrived data and changing circumstances.
- **Re-adjusts risk baselines** by sensing ("observation") of external environment and a cognitive process of "orientation", to make optimal decision.
- Observation works with **outside- in sensory information**, orientation works with **inside-out created operational condition configurations**, that might contain cognitive bias, but can also work better with uncertainties, partial information, diversity or degree of randomness and disorder.
- **Probabilities of a risk vary depending on OBSERVATION and ORIENTATION including OPERATIONAL CONDITIONS,** including sources of data (trust in them), timeliness and other data

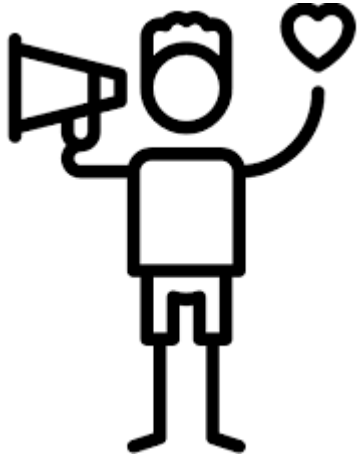
- Focus on cyber risks as a "threat multiplier":



Solutions in SUNRISE

SUNRISE

+ ***Scenarios: adaptivity, collaboration, absenteeism…***
+ ***Technology design, development, piloting and validation***
  - Risk-based access control to protect the essential workers and societies at large
  - Remote physical infrastructure inspection to enable safety of CIs while lacking of human resources
  - Increased cyber-physical resilience to address new threats in remote working conditions
  - Resource demand prediction and management to address the changes in the demand o physical goods
+ ***Awareness and impact creation***
  - Enhance knowledge, awareness and capacities for unity and resilience in Europe



Policy Task Force in SUNRISE

Methodology

- Policy assessment done at **several levels**, in several WP, crossing strategic, tactical, and operational issues
- The SUNRISE Strategy Implementation Process addressing identification of general conditions, but also temporary conditions, together with **possible scenarios potential consequences and available countermeasures**, that include special economic policies to tackle the effect of the pandemic (or other adversary events) or non-pharmaceutical interventions (NPI)
- "Default" EU and CI policies are based on **assumptions about normal or emergency operations**, with a limited number of in-between situations or operational scenarios where collaboration and adaptivity depend on workforce and supply chain availability
- Assessing what worked well in SUNRISE pilots helps **identify "operational level" constraints**, allowing policymakers to revise or update policies for better alignment with different scenarios.
- Understand trade-offs and whether decision and policy makers have time to understand the capabilities, limitations or risks reported from "operational level" due to **dynamic changes in operational conditions**
- Task Force established in June 2024 with representatives from all WP
- Scoring and ranking was done in a collaborative manner to prioritize and focus on specific findings that might have impact on policy

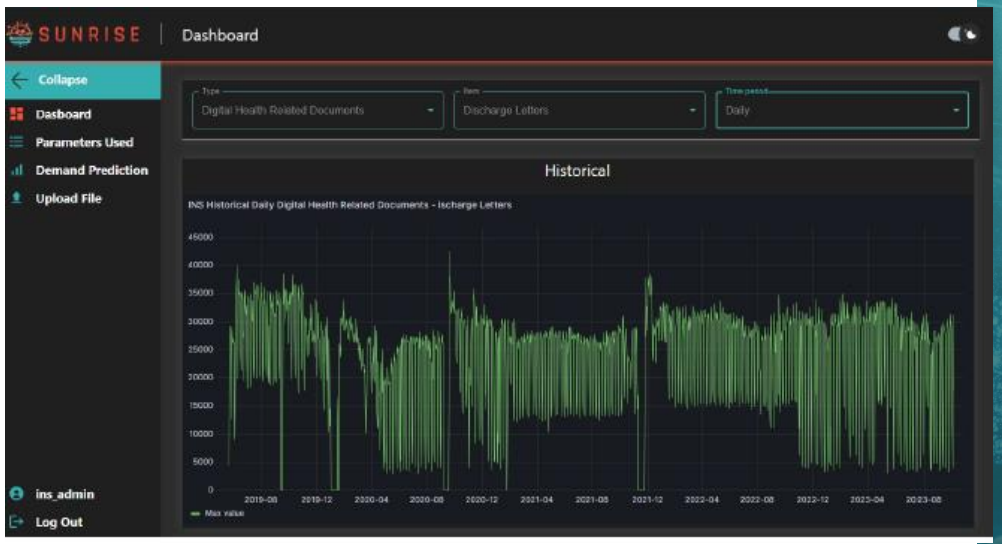
Findings and link to SUNRISE work

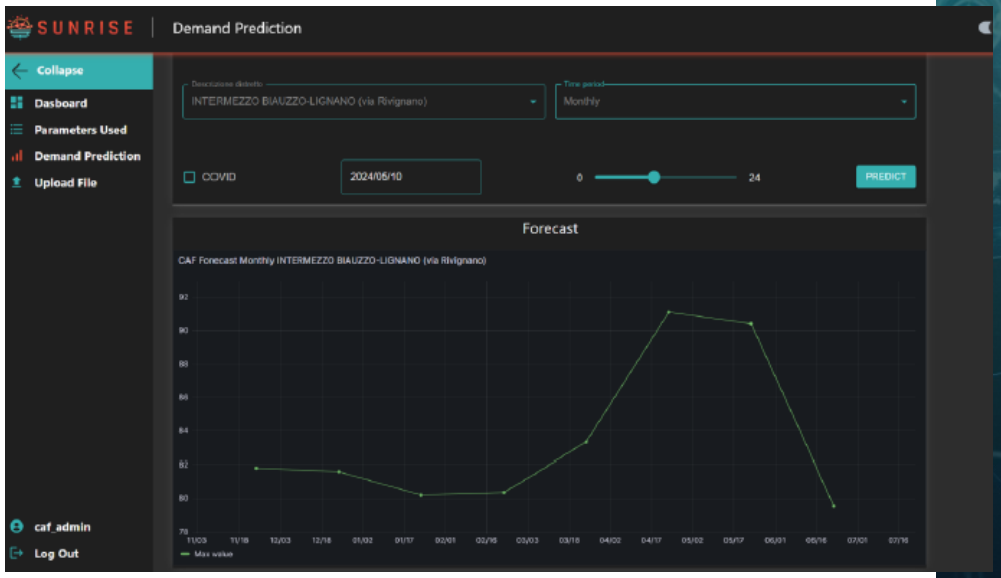
SUNRISE

- **Scenario based planning** to improve dynamic orientation: implementing an automated integration between the Risk Assessment Tool, What If Analysis and Cascading Effects Simulation: what would next pandemics look like?
  - CI profiles recorded via the Risk Assessment Tool will be automatically and periodically exported to form a network of PSCEs (pandemic-specific critical entities) and their relations between each other.
  - The What If simulation (technically planned as an *i-frame* integration directly inside the Risk Assessment Tool) then provides results
- **Data driven decision making** to improve dynamic observation
  - Integration of external data (e.g. threat intelligence sharing incl trust score and relevance) to adapt probability dynamically
  - Integration of real-time data
  - Integration of temporary condition variables (e.g., change of priority that changes impact in risk assessment)
  - Resource availability (data, human, supply chain…), Demand prediction

Demand Prediction and Management (DPM) Tool

1. Societal stability during pandemics
2. Contributes to strategic decision-making in business and government
3. Utilizes climate and weather data for a holistic macroeconomic impact
4. Adaptation to changing demands for economic resilience
5. Minimization of disruptions to critical services





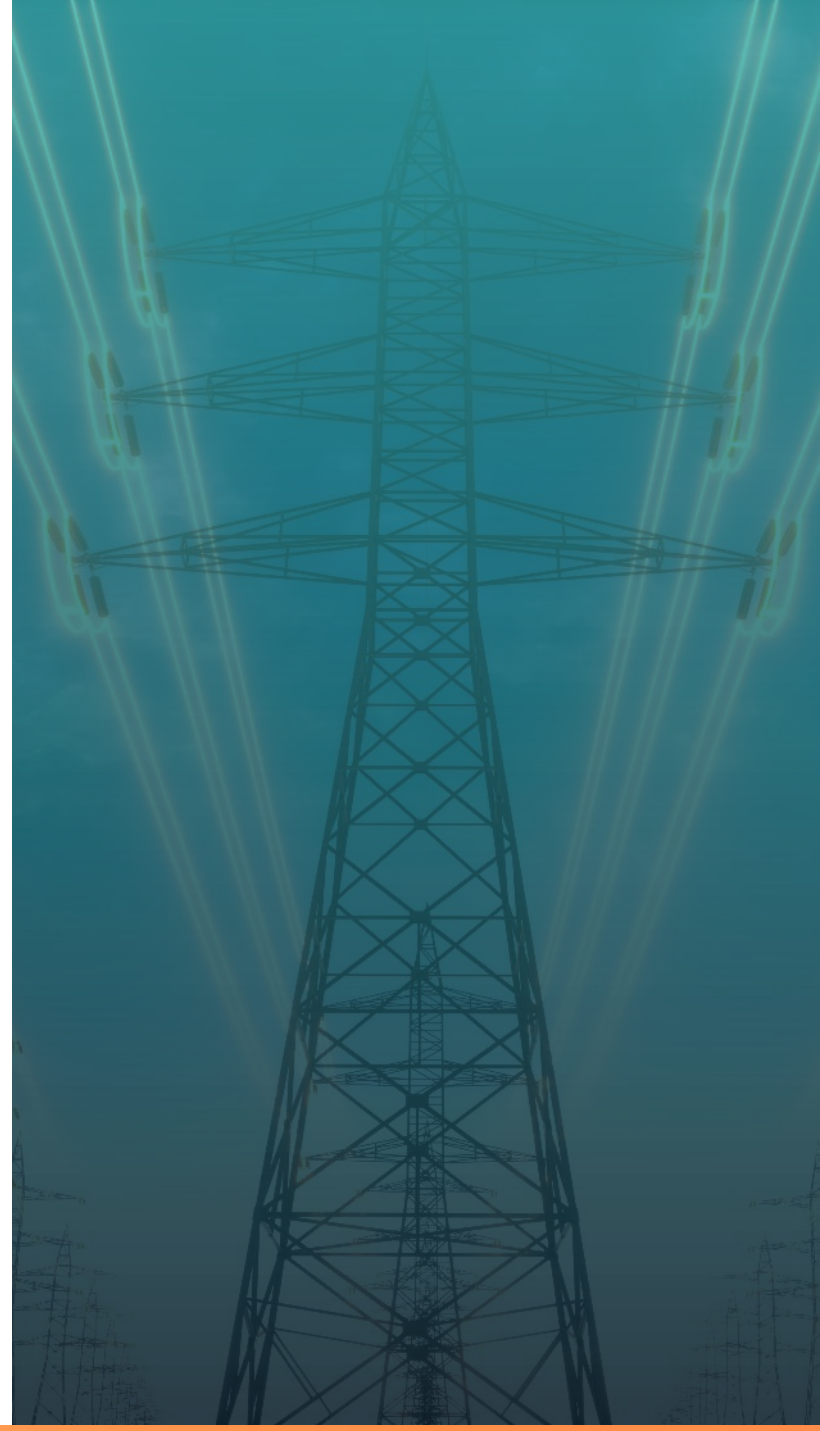
Other issues in Policy Support Taskforce

- Focus on DYNAMIC conditions of each CI: Practicable definitions and criteria to characterize CIs or CEs during a temporary event e.g., specific pandemic. What parts of temporary conditions are **generic and applicable to all CI operators from all sectors, and which parts are specific** for sector or CI operators?

- Focus on DURING phase: Broader definition of resilience: not only limited to the ability to recover or “bounce back” from a perturbation such as a pandemic, i.e., involving post-incident activities, but also pre-emptive activities and measures before the incident, as well as **concurrent activities while the incident is happening.**

- Focus on “CROSS” feature of EU policies: **Integration or interoperability** of SUNRISE strategy process with already existing risk management processes, and frameworks for assessing pandemics

- In case of pandemic, is 100% NIS2 or CER compliance more important than other priorities?



Conclusions

SUNRISE: model, share, control, predict, detect

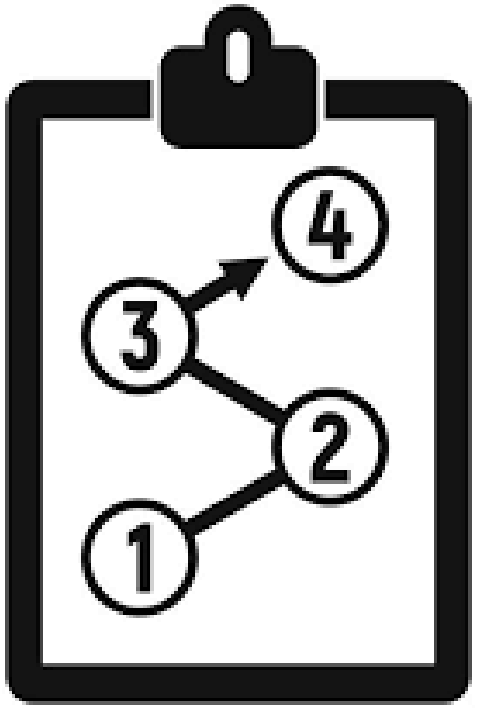
SUNRISE

- Lessons learned from COVID-19:
  - Need for adaptivity (dynamic impact assessment, dynamic changes of probability of adverse events, risks derived from new mitigation measures e.g. NPI)
  - Need for better collaboration
    - vertical – between govt levels and CI operators
    - horizontal operational level between sectors
  - Need to use real-time and external data for monitoring risk evolution and context/scenario changes (e.g., resource availability, demand prediction, threat landscape)

- "Threat multipliers" and Multi-hazard scenarios: human factors (absenteeism, stress…), supply chain disruptions, cyber-physical attacks…
- Cross-sector and cross-EU dependencies: cascading effects, collaboration dynamicity, trust erosion…
- Continuous resilience management: monitor attack vectors, derived risks, reasoning with uncertain/missing data, use of real time data, anomaly detection, etc

From lessons learned to policy inputs

- *We have many lessons from pandemics, but gaps in CI resilience and protection still need to be addressed*
- *Dynamic contextualization (for outside-in sensing), but also context adaptation (inside-out decisions) need both scenario-based planning (BEFORE) and data driven decision making (DURING)*
- *Considering CI technology, people, and processes at operational level and in temporary operational conditions (e.g., pandemics or any "threat multiplier" scenarios) is a key for stress testing of resilience of CI*



SUNRISE

Thank you for your time

Any Questions?

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101073821