Current and emerging risks and challenges for CIP/CIR – assessment of threats, gaps and needs

Chair: Prof. Dr. Aleksandar Jovanović, CEO, Steinbeis European Risk & Resilience Institute

Irene Bonetti, Attilio Carmagnani "AC" SpA

Frédéric Guyomard, Électricité de France (EDF)

Frederic Petit, European Commission Joint Research Centre

Nikolaos Papagiannopoulos, Athens Airport

Vito Morreale, Engineering Ingegneria Informatica S.p.A.

EU-CIP Project & ECSCI Cluster 1st Annual Conference
on Critical Infrastructure Resilience

"Reinventing European resilience"

EU-CIP
RESILIENCE

Roundtable #1: Emerging risks & CIP/CIR

Moderator: A. Jovanovic
(Steinbeis EU-VRi European Risk & Resilience Institute)

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

Agenda & Panelists

10.45-12.15	**Roundtable #1:** Current and emerging risks and challenges for CIP/CIR – assessment of threats, gaps and needs

10:45-10:55
Moderator's introduction – Why "preparing for the unknowns" is so important – slides, the questions one will try to address during the discussion (10')

INTRODUCTION OF THE PANELISTS (1'each)

- Panelist 1: Irene Bonetti, Chemical CI, Italy
- Panelist 2: Nikos Papagiannopoulos, Airport, Greece
- Panelist 3: Frédéric Guyomard, Energy supply, France
- Panelist 4: Gabriele Giunta >> Vito Morreale, The EU-project side
- Panelist 5: Frédéric Petit, The EU/EU-research side

11:00-12:00
PANELISTS TALKS POSSIBLY ADDRESSING MODERATOR's QUESTIONS BELOW
(8' talk, supported or not by the slides, + 4' discussion)

General discussion (15')

Closure – the takeaway message(s)?

Panelist 1: Irene Bonetti

The "smaller" critical infrastructure side, chemical plant

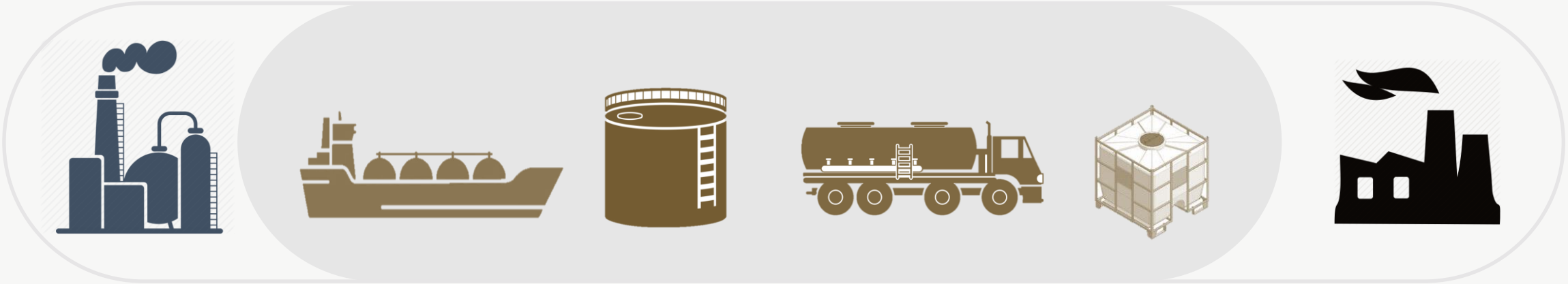
- What "emerging risks/threats" do we talk about in a critical infrastructure like Carmagnani?
- How to strike a balance among:
  - Compliance ("old" risks) and voluntary prevention ("new" risks, still not covered by regulations) – e.g. how to justify investment beyond compliance? How to prove that it was useful and necessary?
  - Economic pressure and investment in safety (e.g. how to justify the higher cost of safer product if the "upfront safety" is not required/recognized by the market)
  - Internal and external investing in people and competencies needed (e.g. should one employ an own AI person or use the 3rd party service?)
- What kind of support is needed on the EU and national side?
- Concerns/ideas, not mentioned above

ATTILIO CARMAGNANI "AC"
Since 1904

Irene Bonetti
Terminal manager Attilio Carmagnani "AC" SpA receipt, storage and forwarding by road, rail and sea of chemicals and petrochemicals products.
It is a SEVESO infrastructure.
I manage, plan and control logistic, maintenance and technical activities of the terminal.
I am responsible for safety, security, environment.

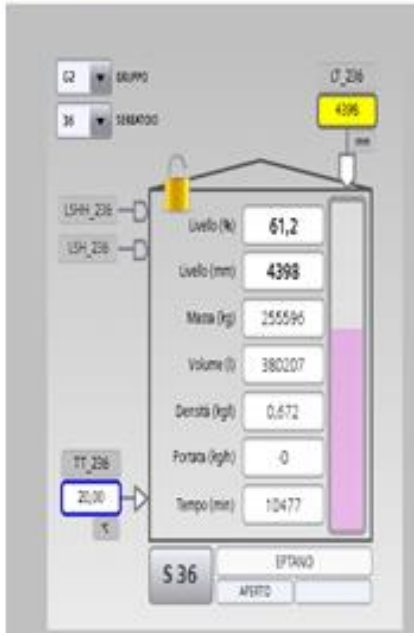
Member of Attilio Carmagnani "AC" SpA board and of Analisi & Controlli Srl board.
Member of the General Council of Confindustria Genoa,
President of Group of Chemical, Oil and Energy entreprises "CHENPE" of Confindustria Genoa ,
Vice President of SMEs Confidustria Genoa.
Member of Confindustria Group for Research and Innovation.
Italian representative for Unione Petrolifera in FETSA (Federation of the European Tanks Storage Associations), board member .
Coordinator and partner in several innovation research projects KARMA ; EU projects INFRASTRESS, FESR, Industry 4.0.

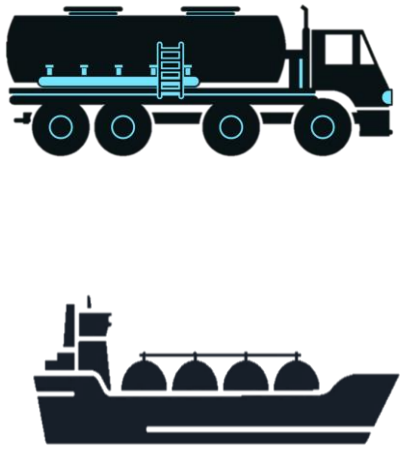
SUPPLY CHAIN PROCESS



The process

ATTILIO CARMAGNANI "AC"

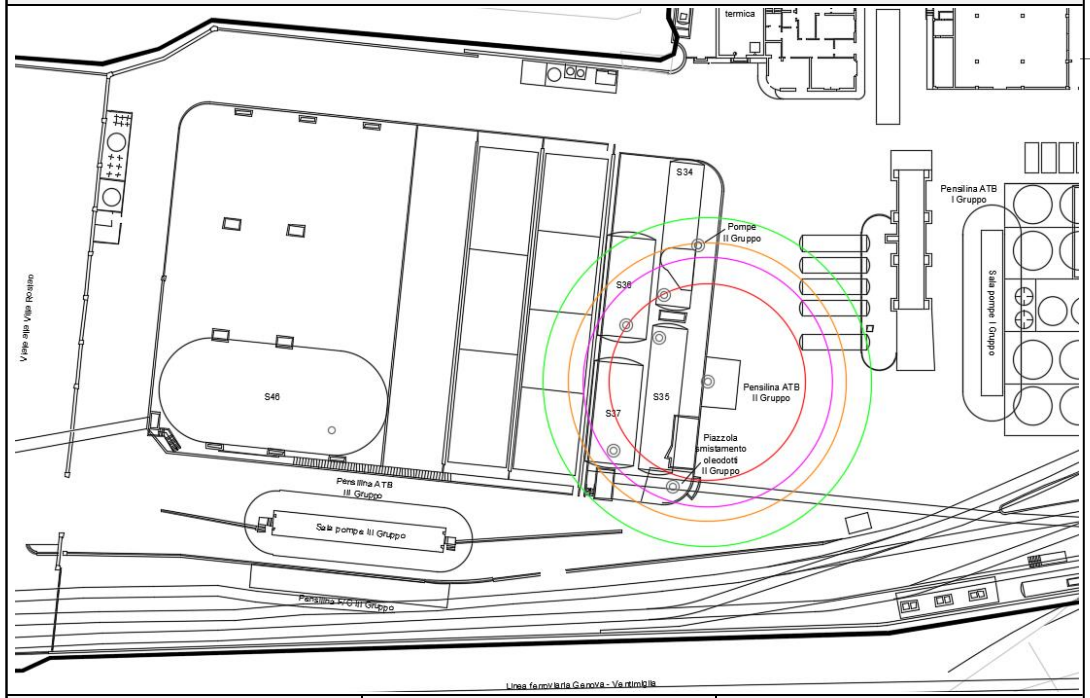




Propriety: Combustion, thermic stability, deflagration, detonation, toxicity , …
System security: design, affidability, process engineering, organization, resilience …
Risk analysis: Loss prevention. quantity analysis, decision analysis, NaTech event, domino effect, …

Risks

TRUCK OVERFLOW DURING LOADING

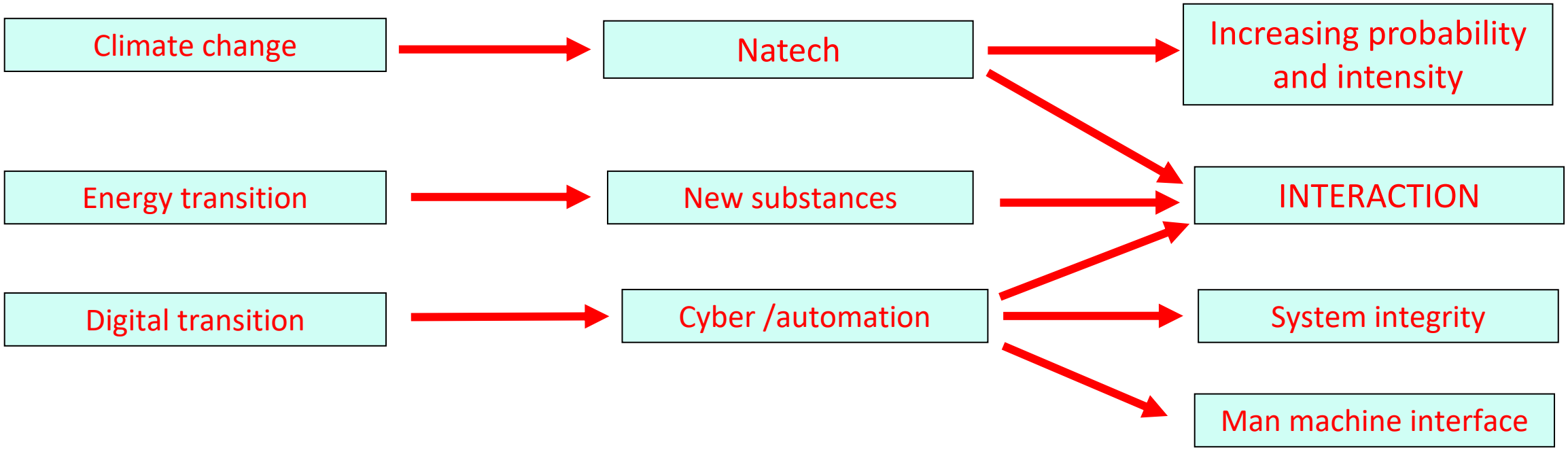


INCIDENTAL SCENARIO	ENERGY TRESHOLD	DAMAGE DISTANCE
POOL FIRE	12,5 KW/m^2	14 m
	7 KW/m^2	17 m
	5 KW/m^2	19 m
	3 KW/m^2	23 m

Loss of containment of dangerous substances mainly solvents

- Pollution
- Toxic plumes
- Pool Fire and flash fire
- Explosion

Emerging risks



Risk assesment

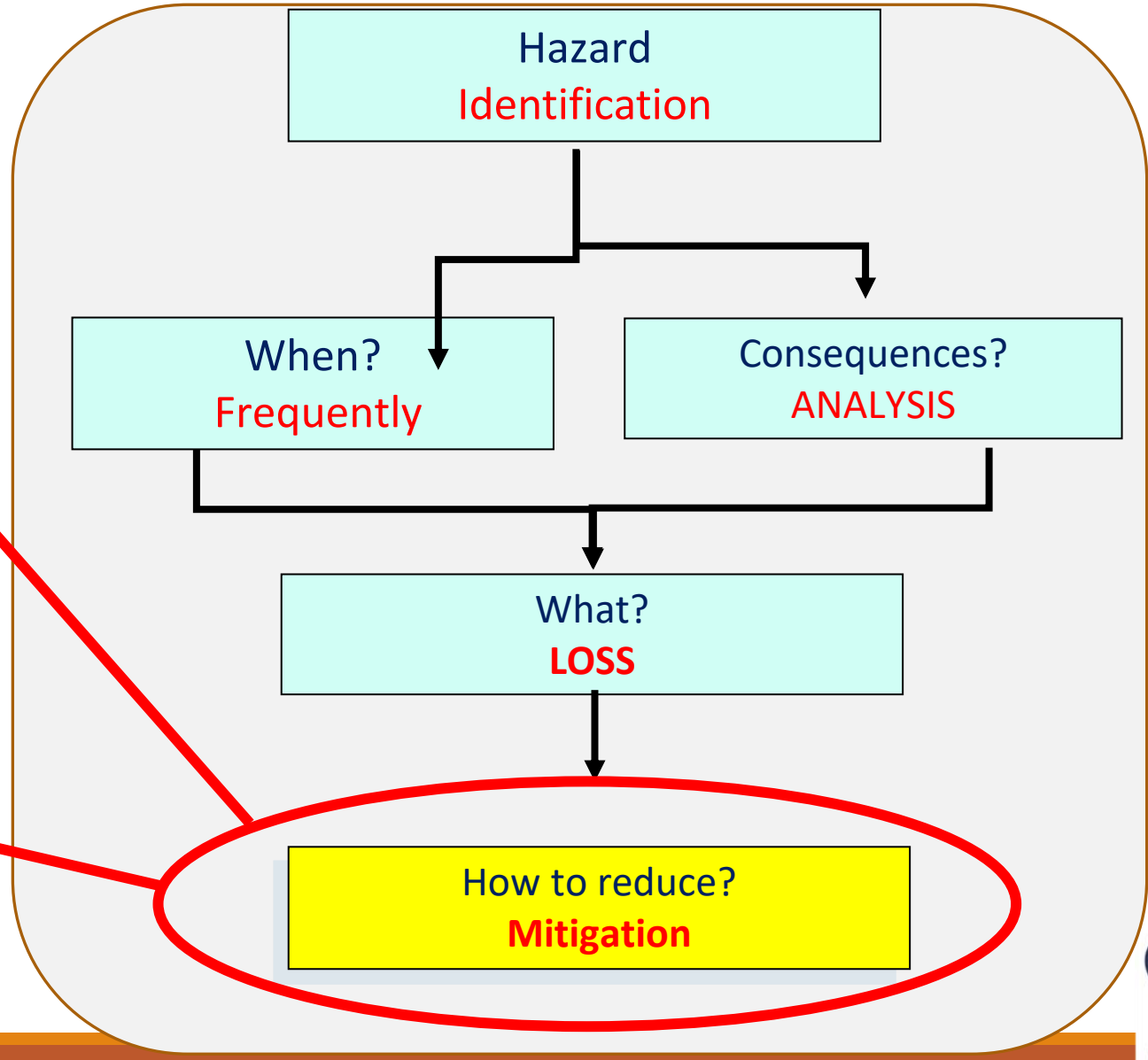
Old risks

Compliance to regulation

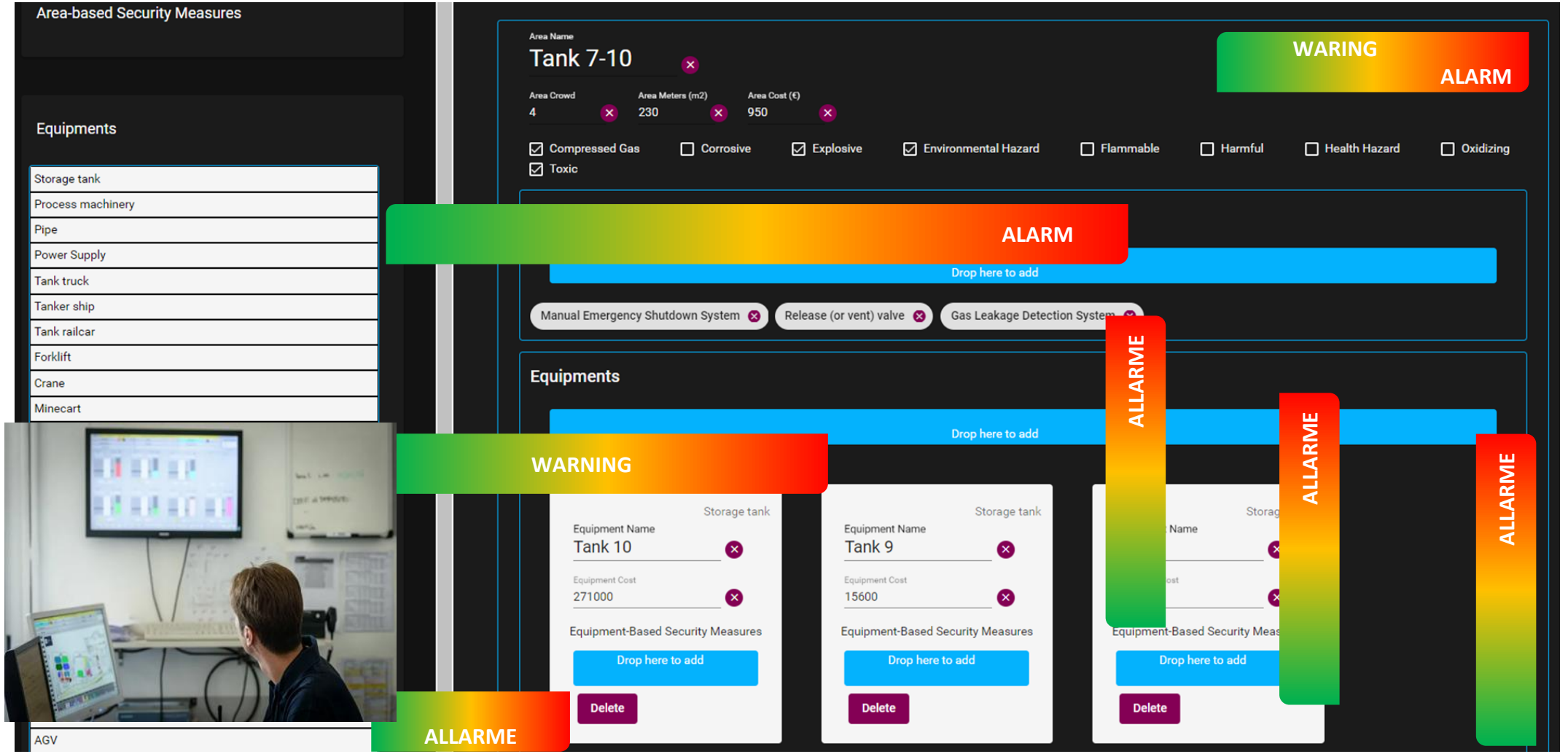
New risks

Loss/investment (beyond compliance) = ?

Corporate sustainability



Competence needed: software data management, alarm handling - unit – system test upgrade, reliability.



What support do we need

- Clear rules
- Standards
- Procedures taking in account transition
- Civil servants well prepared
- Education and traning LLL
- Data sharing interface

Thank you

Panelist 2: Nikos Papagiannopoulos

Dealing with multiple and compound emerging risks in critical infrastructure operation? Airport…

- Emerging risks related to SAFETY
- Emerging risks related to SECURITY
- How to prioritize short and long-term risk mitigation measures? Who is supporting/financing/praising the long-term investments?
- Panelist's concerns/ideas, not mentioned above

Panelist 3: Frederic Guyomard

The national mission-critical infrastructure side? Energy…

Which “emerging risks/threats” do we talk about in an industry like EDF? Ok can be covered, (Cosmic Energy – Industroyer 2, Ransomware).

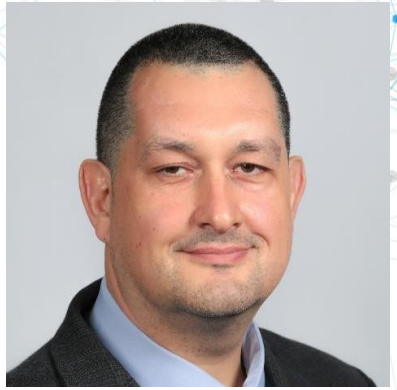
- How to cope with:
- Changing EU and national requirements? Can be Covered with CER – CRA – Network Code
- Extreme crises: COVID, wars, supply chain… Ok can be covered, Quickly adapt the organization
- Who should pay for the “enhanced resilience” of critical infrastructure? Ok can be covered
- Are nationally/EU mission-critical infrastructures well supported? Where are the gaps and possible improvements Not easy to cover, maybe a to large subject
- Do the EU project provide the help which is needed? Ok can be covered
- Open question : How to facilitate More collaboration again for example by joining the European Institutes
- A European Operational Center to cover Major Cyber Security Incident – Crisis management and global risk for CI?
- Panelist’s concerns/ideas, not mentioned above

Panelist 4: Vito Morreale

The EU project side? Engineering consultant company…

- Examples from current projects
- Do we have enough involvement of industry?
- What kind of improvement is needed/possible?
- Panelist's concerns/ideas, not mentioned above

Panelist 5: Frederic Petit



The EU side? EU Joint Research Center (JRC)…

- General goals in the area of CIPs: CER Directive and beyond? Other directives?
- JRC: Link between resilience and the threats? Stress-testing?
- JRC: Use of resilience indicators? Don’t we need them? How should that work in the “EU decentralized safety/security environment”?
- Exchange of sensitive data?
- Panelist's concerns/ideas, not mentioned above

CIP & CIR Assessments

Roundtable # 1

1st Annual Conference on Critical Infrastructure Resilience

19th September 2023, Brussels

Frédéric Petit

Directorate E: Space, Security and Migration

Unit E.2: Technology Innovation in Security

Joint Research Center

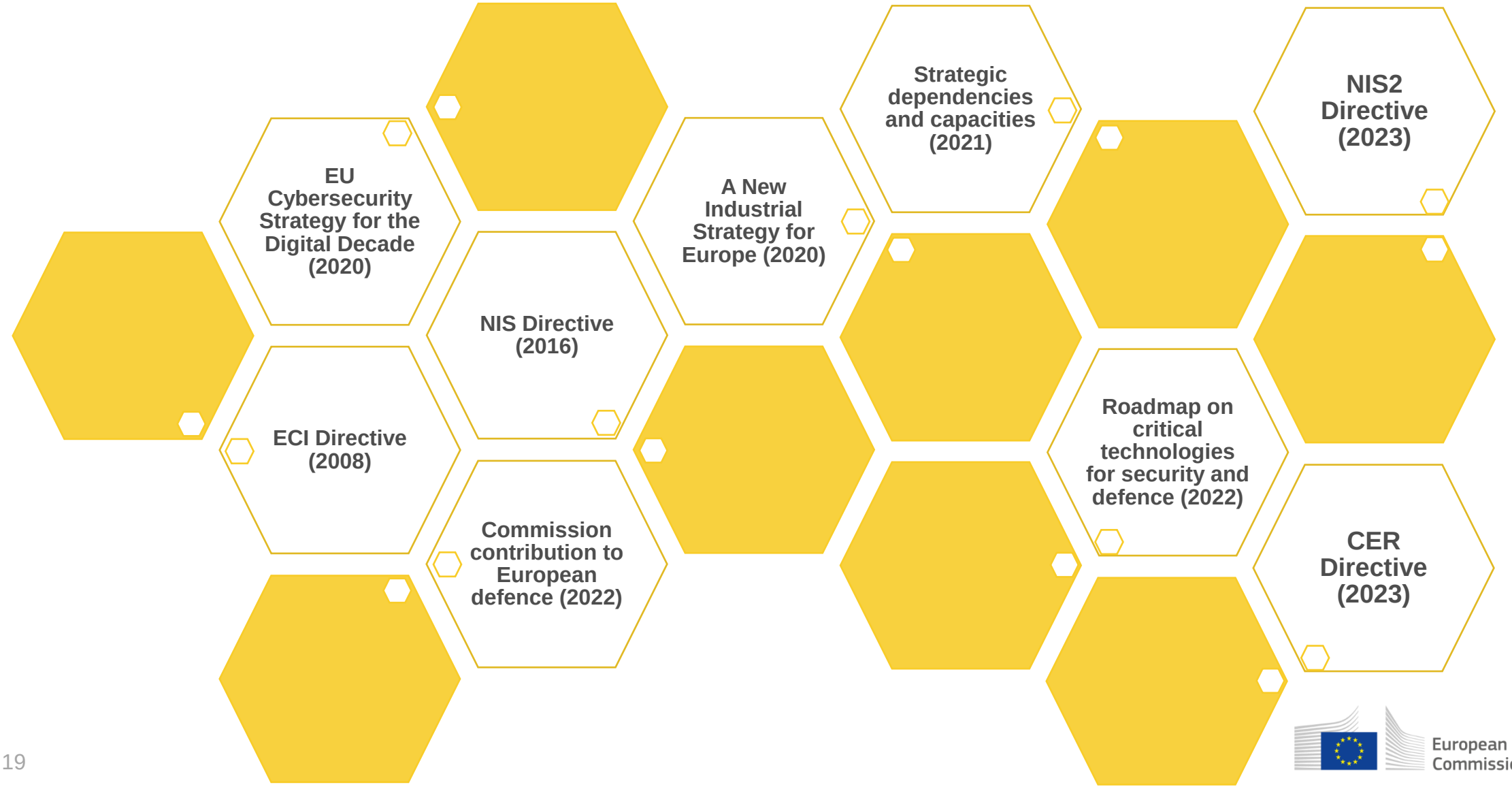
Frederic.PETIT@ec.europa.eu

European Commission

Outline

- EU Directives
- Use of Resilience Indicators
- What is happening outside the EU?
- European Reference Network for Critical Entities Resilience
- Addressing the challenges

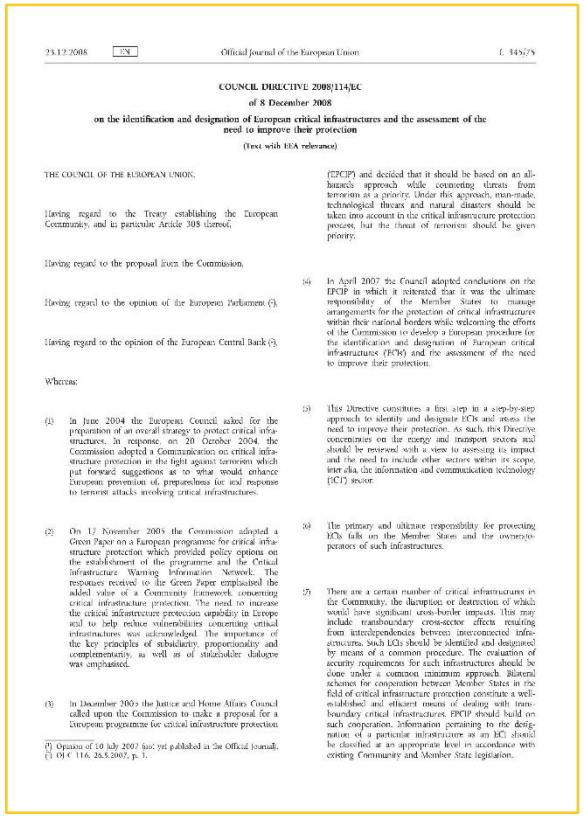
EU Policies affecting CI



European Commission

Paradigm shift

COUNCIL DIRECTIVE 2008/114/EC



23.12.2008 EN Official Journal of the European Union L 345/75

COUNCIL DIRECTIVE 2008/114/EC
of 8 December 2008
on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
(Text with EEA relevance)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 308 thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Parliament (1),

Having regard to the opinion of the European Central Bank (2),

Whereas:

(1) In June 2004 the European Council asked for the preparation of an overall strategy to protect critical infrastructures. In response, on 20 October 2004, the Commission adopted a Communication on critical infrastructure protection in the fight against terrorism which put forward suggestions as to what would enhance European prevention of, preparedness for and response to terrorist attacks involving critical infrastructures.

(2) On 17 November 2005 the Commission adopted a Green Paper on a European programme for critical infrastructure protection which provided policy options on the establishment of the programme and the Critical Infrastructure Warning Information Network. The responses received to the Green Paper emphasised the added value of a Community framework concerning critical infrastructure protection. The need to increase the critical infrastructure protection capability in Europe and to help reduce vulnerabilities concerning critical infrastructures was acknowledged. The importance of the key principles of subsidiarity, proportionality and complementarity, as well as of stakeholder dialogue was emphasised.

(3) In December 2005 the Justice and Home Affairs Council called upon the Commission to make a proposal for a European programme for critical infrastructure protection (EPCIP) and decided that it should be based on an all-hazards approach while countering threats from terrorism as a priority. Under this approach, man-made, technological threats and natural disasters should be taken into account in the critical infrastructure protection process, but the threat of terrorism should be given priority.

(4) In April 2007 the Council adopted conclusions on the EPCIP in which it reiterated that it was the ultimate responsibility of the Member States to manage arrangements for the protection of critical infrastructures within their national borders while welcoming the efforts of the Commission to develop a European procedure for the identification and designation of European critical infrastructures (ECIs) and the assessment of the need to improve their protection.

(5) This Directive constitutes a first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection. As such, this Directive concentrates on the energy and transport sectors and should be reviewed with a view to assessing its impact and the need to include other sectors within its scope, inter alia, the information and communication technology (ICT) sector.

(6) The primary responsibility for protecting ECIs falls on the Member States and the owners/operators of such infrastructures.

(7) There are a certain number of critical infrastructures in the Community, the disruption or destruction of which would have significant cross-border impacts. This may include transboundary cross-sector effects resulting from interdependencies between interconnected infrastructures. Such ECIs should be identified and designated by means of a common procedure. The evaluation of security requirements for such infrastructures should be done under a common, minimum approach. Bilateral schemes for cooperation between Member States in the field of critical infrastructure protection constitute a well-established and efficient means of dealing with trans-boundary critical infrastructures. EPCIP should build on such cooperation. Information pertaining to the designation of a particular infrastructure as an ECI should be classified at an appropriate level in accordance with existing Community and Member State legislation.

(1) Opinion of 10 July 2007 (not yet published in the Official Journal).
(2) OJ C 116, 26.5.2007, p. 1.

Critical Infrastructures → **Protection**

Critical Entities → **Resilience**

DIRECTIVE (EU) 2022/2557

L 333/164 EN Official Journal of the European Union 27.12.2022

DIRECTIVE (EU) 2022/2557 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 14 December 2022
on the resilience of critical entities and repealing Council Directive 2008/114/EC
(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the Committee of the Regions (2),

Acting in accordance with the ordinary legislative procedure (3),

Whereas:

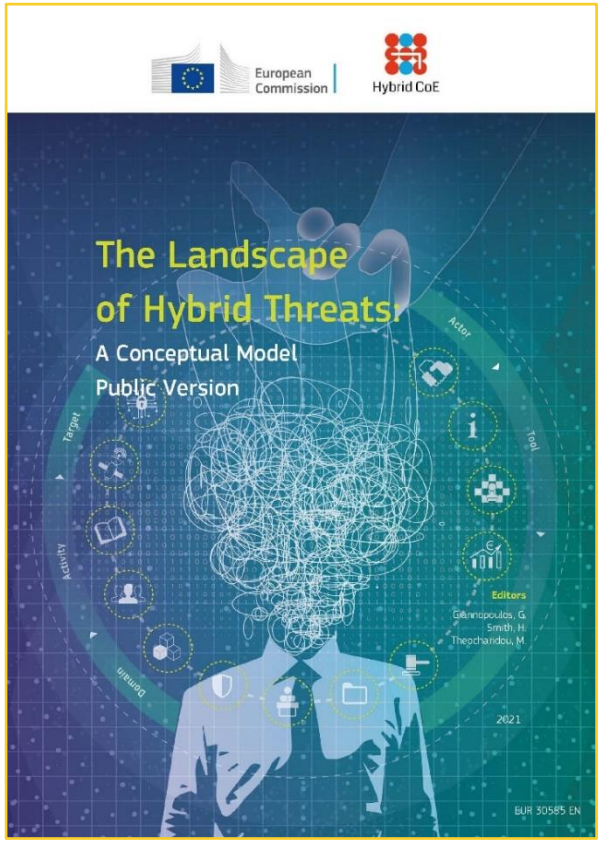
(1) Critical entities, as providers of essential services, play an indispensable role in the maintenance of vital societal functions or economic activities in the internal market in an increasingly interdependent Union economy. It is therefore essential to set out a Union framework with the aim of both enhancing the resilience of critical entities in the internal market by laying down harmonised minimum rules and assisting them by means of coherent and dedicated support and supervision measures.

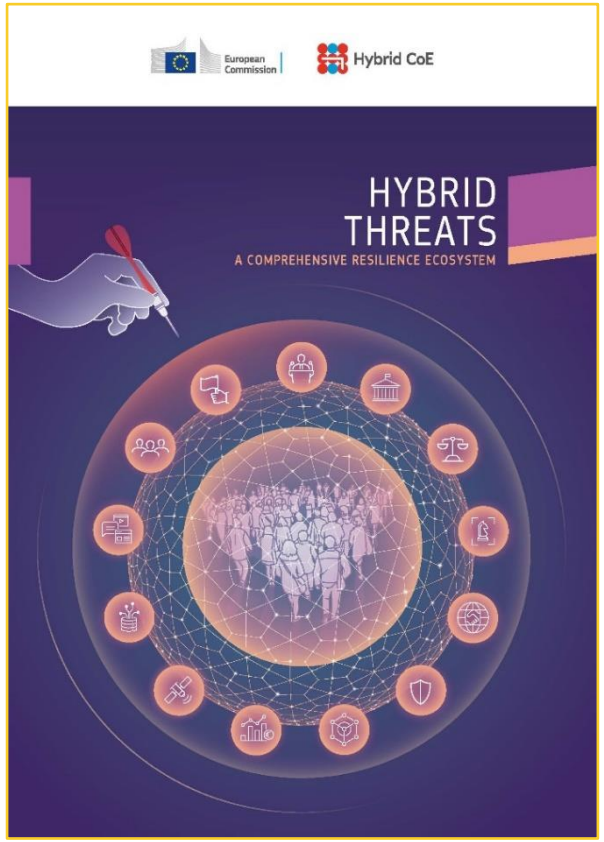
(2) Council Directive 2008/114/EC (4) provides for a procedure for designating European critical infrastructure in the energy and transport sectors the disruption or destruction of which would have a significant cross-border impact on at least two Member States. That Directive focuses exclusively on the protection of such infrastructure. However, the evaluation of Directive 2008/114/EC conducted in 2019 found that, due to the increasingly interconnected and cross-border nature of operations using critical infrastructure, protective measures relating to individual assets alone are insufficient to prevent all disruptions from taking place. Therefore, it is necessary to shift the approach towards ensuring that risks are better accounted for, that the role and duties of critical entities as providers of services essential to the functioning of the internal market are better defined and coherent, and that Union rules are adopted

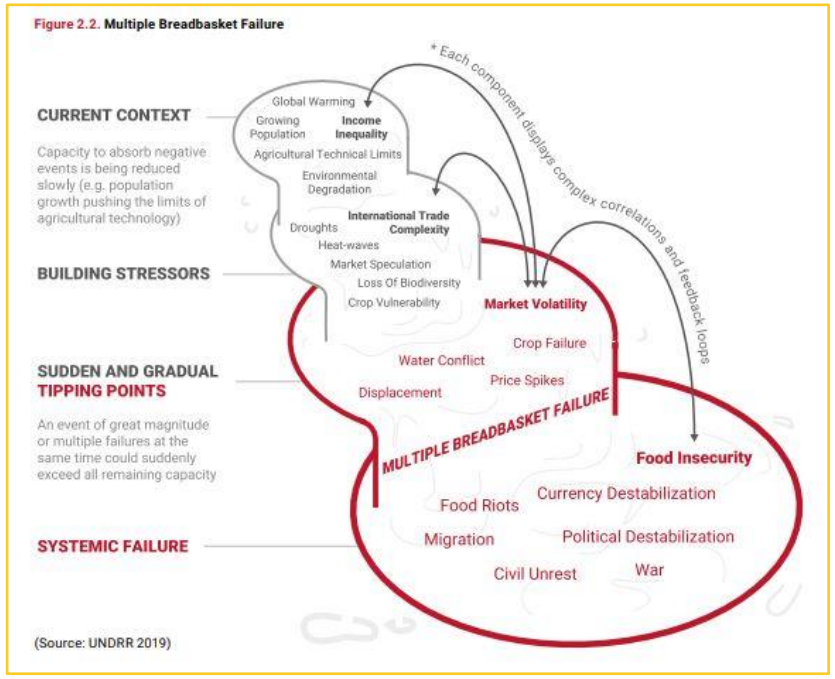
(1) OJ C 286, 16.7.2021, p. 170.
(2) OJ C 440, 29.10.2021, p. 99.
(3) Position of the European Parliament of 22 November 2022 (not yet published in the Official Journal) and Council Decision of 8 December 2022.
(4) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75).

European Commission

Hybrid threats & systemic risk



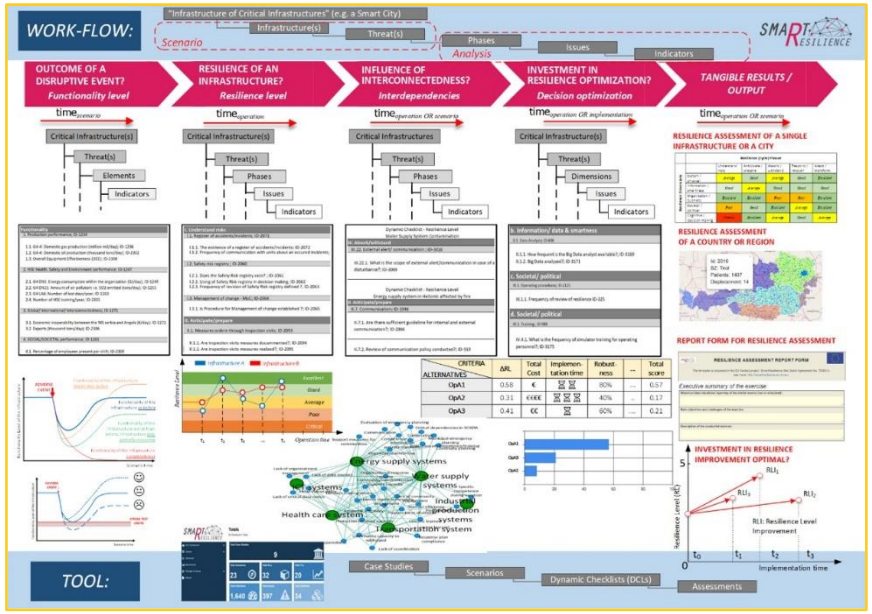


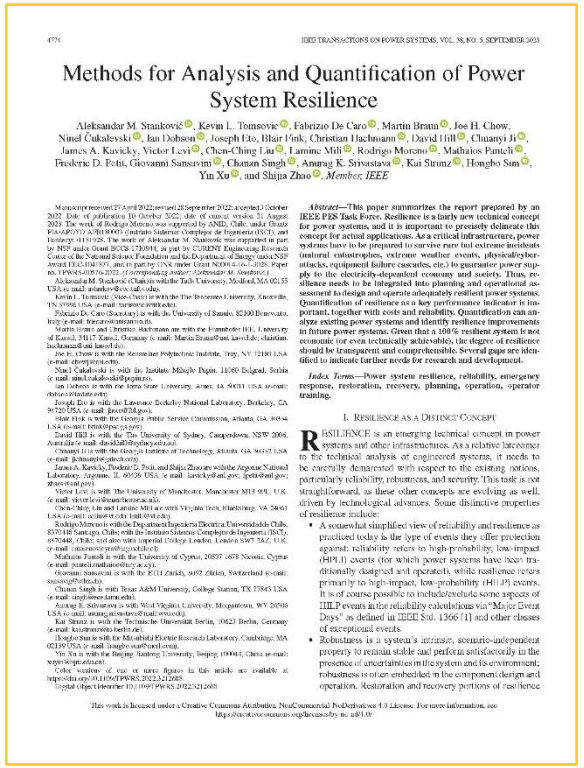


European Commission

Resilience indicators

- Helpful for technical and non-technical audiences
- Must provide meaningful and truthful information
- Must be transparent, defensible, repeatable





Methods for Analysis and Quantification of Power System Resilience

Aleksandar M. Stanković, Kevin L. Tomsovic, Fabrizio De Caro, Martin Braun, Joe H. Chow, Nimet Čukalevski, Ian Dobson, Joseph Eto, Blair Fink, Christian Hachmann, David Hill, Chuanyi Ji, James A. Kavicky, Victor Levi, Chen-Ching Liu, Lamine Mili, Rodrigo Moreno, Mathaios Panteli, Frederic D. Petit, Giovanni Sansavini, Chanan Singh, Anurag K. Srivastava, Kai Strunz, Hongbo Sun, Yin Xu, and Shijia Zhao, *Member, IEEE*

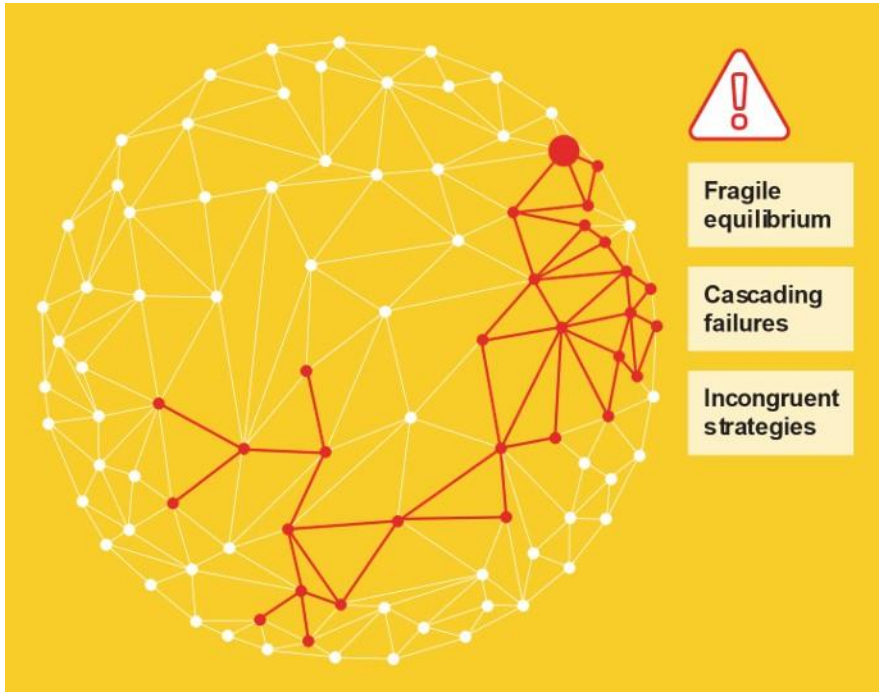
Abstract—This paper summarizes the report prepared by an IEEE PES Task Force. Resilience is a fairly new technical concept for power systems, and it is important to precisely delineate this concept for actual applications. As a critical infrastructure, power systems have to be prepared to survive rare but extreme incidents (natural catastrophes, extreme weather events, physical/cyber-attacks, equipment failure cascades, etc.) to guarantee power supply to the electricity-dependent economy and society. Thus, resilience needs to be integrated into planning and operational assessment to design and operate adequately resilient power systems. Quantification of resilience as a key performance indicator is important, together with costs and reliability. Quantification can analyze existing power systems and identify resilience improvements in future power systems. Given that a 100% resilient system is not economic (or even technically achievable), the degree of resilience should be transparent and comprehensible. Several gaps are identified to indicate further needs for research and development.

Index Terms—Power system resilience, reliability, emergency response, restoration, recovery, planning, operation, operator training.

I. Resilience as a Distinct Concept

Resilience is an emerging technical concept in power systems and other infrastructures. As a relative latecomer to the technical analysis of engineered systems, it needs to be carefully demarcated with respect to the existing notions, particularly reliability, robustness, and security. This task is not straightforward, as these other concepts are evolving as well, driven by technological advances. Some distinctive properties of resilience include:

- A somewhat simplified view of reliability and resilience as practiced today is the type of events they offer protection against: reliability refers to high-probability, low-impact (HILP, I) events (for which power systems have been traditionally designed and operated), while resilience refers primarily to high-impact, low-probability (HILP) events. It is of course possible to include/exclude some aspects of HILP events in the reliability calculations via "Major Event Days" as defined in IEEE Std. 1366 [1] and other classes of exceptional events.
- Robustness is a system's intrinsic, scenario-independent property to remain stable and perform satisfactorily in the presence of uncertainties in the system and its environment; robustness is often embedded in the component design and operation. Restoration and recovery portions of resilience



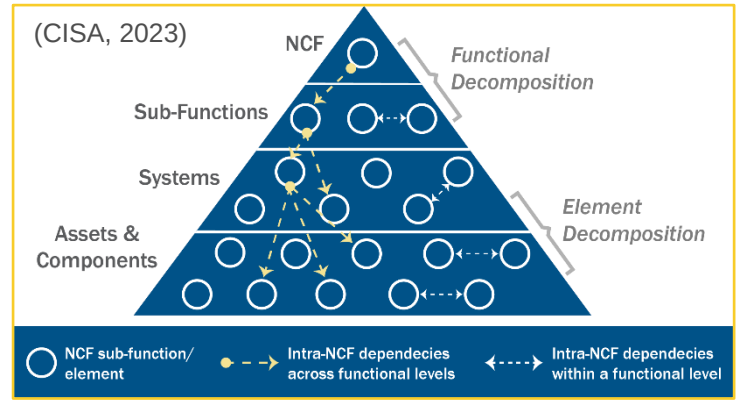
"Everything that can be counted does not necessarily count; everything that counts cannot necessarily be counted."

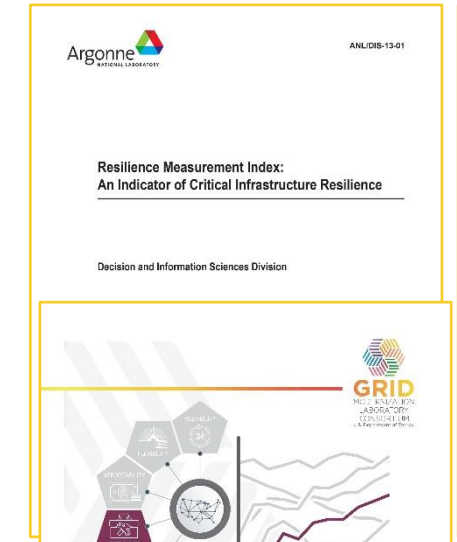
Albert Einstein

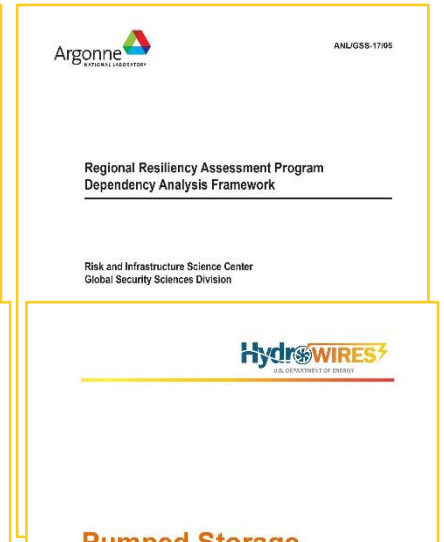
European Commission

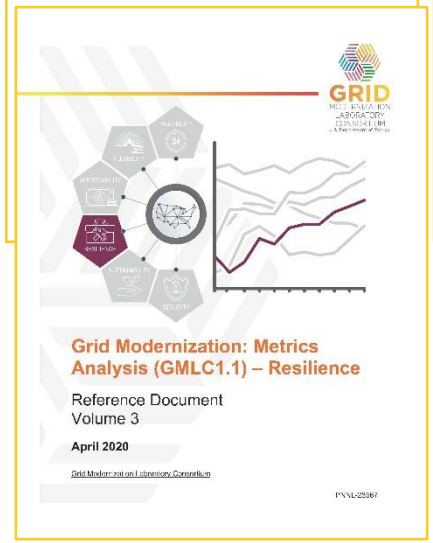
Outside the EU

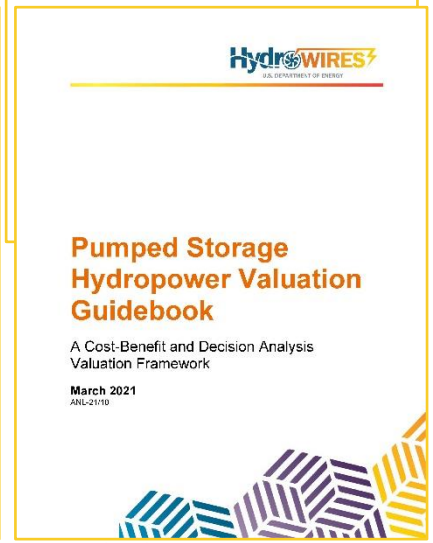
- Presidential Policy Directive (PPD21) on Critical Infrastructure Security and Resilience
- Executive Order (EO) 14028 on Improving the Nation's Cybersecurity
- Critical Infrastructure and National Critical Functions
- Infrastructure Survey Tool (IST) & Regional Resiliency Assessment Program (RRAP)
- Protected Critical Infrastructure Information (PCII) Program











European Commission

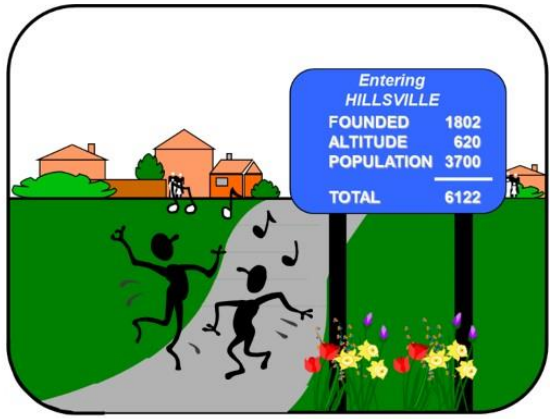
European Reference Network for Critical Infrastructure Protection (ERNCIP)

- Improve **protection and resilience** of critical infrastructures in Europe
- **Collaboration** with CIP stakeholders focusing on technical protection and resilience solutions
- Thematic groups (TGs) to improve the development and availability of **security solutions** through common testing protocols, standardisation and guidelines
- Workshops, trainings and webinars to improve **dissemination** and raise **awareness**

➡ ***Transition to focus on CER***

Addressing the challenges

- Resilience assessment requires multidisciplinary and cooperative efforts
- Critical thinking and imagination are key
- No easy solution – no magic button
- No approach fits every scenario – different needs require different approaches
- Data availability, discrepancies present challenges to manage
- A defensible process is essential to making sound decisions



European Commission

Thank you

European Commission

Discussion

- Questions “parked” during short discussions after panelists’ presentations
- New questions
- Heretic questions: What IS European resilience? What is being “reinvented” in European resilience? What did we get from almost 1,000 EU projects dealing with resilience? Can we rely that “quantity will yield quality”?
- Closure – the 3 main takeaway message(s)? E.g.
  1. We are / we are not well prepared for new/emerging CIP risks/threats?
  2. We have / have not got the full benefit from the EU projects?
  3. We have / have not the “EU way to exchange the sensitive CIP data”?