HORIZONTE EUROPA

HORIZONTE EUROPA CLUSTER 3 (Seguridad civil para la Sociedad):

ayudas a la I+D+i en la Gestión integral de Riesgos, Emergencias, Seguridad y Resiliencia

(contexto: visión integral de PESI hacia la Resiliencia, Retos Twin Transformation e I+D+i en Seguridad)

Jornada SEDEXPO 2023 (Feira Galicia, 29-Nov)

Javier LARRAÑETA
PESI Secretario General
ETPIS Executive Board Officer

tecnalia Inspiring Business

Indice

- Contexto actual: Resiliencia industrial, nuevos riesgos y Twin Transformation (Industry 5.0)
- PESI: Plataforma Tecnológica Española de Seguridad Industrial (seguridad integral, enfoque europeo)
- Ámbitos de Seguridad integral en la Industria 5.0 (Infras 5.0):
  - Seguridad corporativa y Ciberseguridad
- UE: enfoque de la retos Seguridad integral (normativas recientes) y oportunidades tecnológicas en I+D+i

Preámbulo: Resiliencia y accidentes recientes de Seguridad Industrial, nuevos riesgos y Retos (Twin Transformation, Industry 5.0)

Resiliencia y desastres/accidentes industriales: nuevos riesgos y efectos cascada

Desgraciadamente la actividad industrial y económica está plagada de incidentes de diferente naturaleza, gravedad y afección, pero los accidentes industriales acaecidos recientemente conllevan una combinación de nuevos riesgos y situaciones insospechadas con anterioridad:

- **Fukushima: accidente nuclear** derivado de un tsunami provocado por un terremoto, afectando instalaciones críticas (Japón, 11 de marzo de **2011**)
- **Explosión e incendio en el complejo químico de Tarragona (14 enero 2020):** dos trabajadores muertos en planta y un ciudadano en su casa (a 3 Kms del suceso, por el impacto de la tapa del reactor de 1 Tn. que voló hasta un edificio en la población cercana a la fábrica).
- **Ciberataque** (virus WannaCry): paralización durante varios días de servicios centrales de operadores críticos en UE (energía, telecomunicaciones…)
- **PANDEMIA COVID-19** (2020 – actualidad):
  afección global en el funcionamiento de todos los Operadores críticos (incluida la cadena de suministro)

- **Barco embarranca en Canal de Suez (marzo 2021):** paralización del transporte y comercio mundial
- **Invasión y guerra en Ukrania**: **crisis energética, ciberataques** de Rusia a las infraestructuras críticas de los países cercanos al conflicto

Fukushima: accidente nuclear (efectos en cascada)

El tsunami tras el terremoto afecta gravemente a la infraestructura de protección de la instalación y equipamientos (lo que causó la pérdida del suministro eléctrico a la central, y un grave problema de falta de refrigeración del núcleo.
Todos los reactores operativos en las centrales pararon de forma segura, pero los núcleos de los reactores de dos de las unidades se sobrecalentaron, el combustible nuclear se fundió y las tres vasijas de contención se fracturaron. Las explosiones en los edificios de los reactores causaron daños a estructuras y equipo, así como graves lesiones al personal. Posterior contaminación afectando al medioambiente, poblaciones y sus ciudadanos.

El accidente nuclear de Fukushima (11 de marzo 2011) es un fatal ejemplo de las consecuencias de un conjunto de efectos en cascada:

- Desastre natural
- Afección a la instalación industrial (fallos de fiabilidad y en los sistemas de seguridad)
- Sistemas industriales (SCADA) no pueden revertir el proceso
- Accidente industrial grave (derivado en desastre nuclear)
- Pérdidas humanas y materiales
- Afección al Medio Ambiente
- Afección a otras Infraestructuras
- Afección reputacional

Fukushima: nuclear accident or the perfect example of dependencies and cascading effects ?

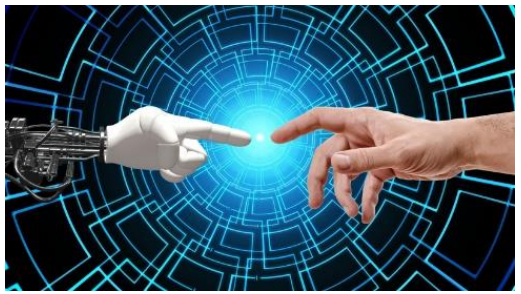
#	Accident steps / Effects	Critical element	Dependency (Intra/Inter)
1	Hearthquake and tsunami (Nature& Climate)	Location of CI	Interdep.
2	Wave destroy coastal infrastructures	Transport infra Energy grid	Interdep.
3	Wave overpass the protection walls of Nuclear plant	Walls (exter-nal perimet)	Intra
4	Water affects electrical appliances (techical failure)	Critical facilities	Intra
5	Cooling system does not work properly (industrial accident)	Critical process	Intra
6	Emergency Team can not avoid the accident nor 1st Responders Access to installations	Team (O&M, external Emergencies)	Intra
7	Control Room cannot stop reactors (heating): Nuclear accident	Critical process	Intra

Seguridad y Resiliencia industrial: riesgos y efectos en cascada

- Desastres naturales (más frecuentes y de mayor intensidad debido al cambio climático): inadecuada **evaluación de riesgos climáticos y sus efectos** sobre las infraestructuras, instalaciones, operación y servicios esenciales.
- Insuficiente **evaluación de las dependencias** de una instalación, en especial si es crítica, tanto internas como de otras infraestructuras (IC: energía, agua, telecom., transporte…) para evitar/minimizar los **efectos en cascada.**
- Falta de mecanismos eficientes: **alerta temprana, información** y **actuación coordinada entre operadores** (Infraestr. Críticas y/o Servicios esenciales).
- Diversas **causas (ciberataques, ataque terrorista, pandemia, sabotaje, fallos técnicos** de diseño, mantenimiento, errores humanos…) también pueden ocasionar una concatenación de similares consecuencias (**directas** y en las **Cadenas de Valor**)
- Falta de **protocolos de actuación coordinados** ante emergencias **híbridas** simultáneas (industrial y catástrofe natural, Ciberataque, pandemia, guerra…) (sí se dispone de Planes de Protección Civil y ejercicios /simulacros en Ciberseguridad pero de forma independiente)
- Pero en especial: el **FACTOR HUMANO** (propio y de la cadena de valor): Equipos críticos, formación/entrenamiento (Cultura de Seguridad/Ciberseguridad, riesgos Psicosociales)
- Y la **coordinación** de las áreas corporativas: Dirección, Personas, **Sistemas**, Gerencia de Riesgos, O&M, Logística,... **con Seguridad Corporativa y SST**

Nuevos Retos (mundiales, UE): Sociales y Twin Transformation

- Cambio Climático
- Energía y Movilidad
- Recursos naturales y sostenibilidad
- Igualdad en la Sociedad (y género)
- **Transformación Digital (Industria 5.0, UE: KET + Personas, Resiliencia y Sostenibilidad)**



Visión ETPIS / PESI (XV Aniversario)

« Innovación y desarrollo tecnológico (I+D+i) con visión global e integradora de la Seguridad Industrial»

(Safety + Security)

4 áreas de despliegue de PESI:

- Seguridad de procesos e instalaciones
- Seguridad y Salud en el trabajo (Personas)
- Seguridad ambiental (riesgos Cambio Climático)
- Seguridad corporativa de la Empresa (Security-Cyber-Emergencias): Resiliencia

Visión integral: Seguridad y Gobernanza de Riesgos para la Resiliencia

también en Infraestructuras y Servicios

Estrategia de Resiliencia (Inteligencia, Seguridad y Gobernanza, GRC)

Gestión de Procesos y Activos: Fiabilidad y Seguridad en Operación y Mantenimiento (RAMS)

Seguridad Medioambiental (riesgos cambio climático)

Gestión de Emergencias (Planes Autoprotección)

Gerencia de Riesgos y Organización de Seguridad (Continuidad de negocio, protección de intangibles)

Ciberseguridad (IT y OT)

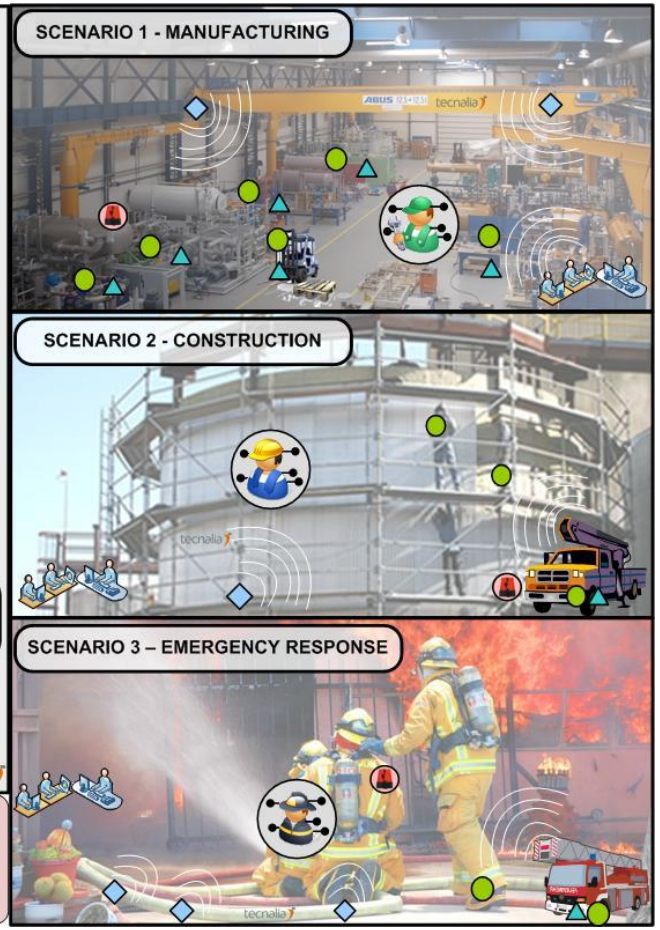
Seguridad Física (Protección de activos físicos y personas)

Factor Humano en Seguridad PIC (Personnel Security)

Seguridad y Salud Laboral
PRL, Bienestar, Adicciones
Movilidad-Seguridad Vial,
Factor Generacional

Entornos inteligentes y seguros de trabajo (por diseño)

Factoría del Futuro (**Industria 4.0/5.0): IA** en apoyo de los EPIs avanzados (Wearables 4.0) y Exoesqueletos, Sensores (IoT), Monitorización (Visión, Bigdata), Robótica colaborativa, Interoperabilidad (servicios de emergencia externos)



Gestión de Riesgos y evolución del concepto clásico de riesgo: nueva ISO y Resiliencia

Concepto tradicional del Riesgo:

- Amenaza / daño – Vulnerabilidad – Consecuencias

Risk Management (ISO 31000)

- enfoque ampliado en Ámbitos
- También en positivo (no sólo en pérdidas): Oportunidades/Beneficios
- **Riesgos Ciber (ISO 2700x)** embebidos

Capacidad corporativa de Resiliencia (concepto avanzado):

- Amenazas/daño – Vulnerabilidad – **Resiliencia** – Consecuencias
- Resiliencia: Procesos/Sistemas/Servicios

Equipo Humano Resiliente (a 2 niveles: Individual y de Equipos): aplicable a la **Ciberseguridad** y **Ciber-resiliencia**

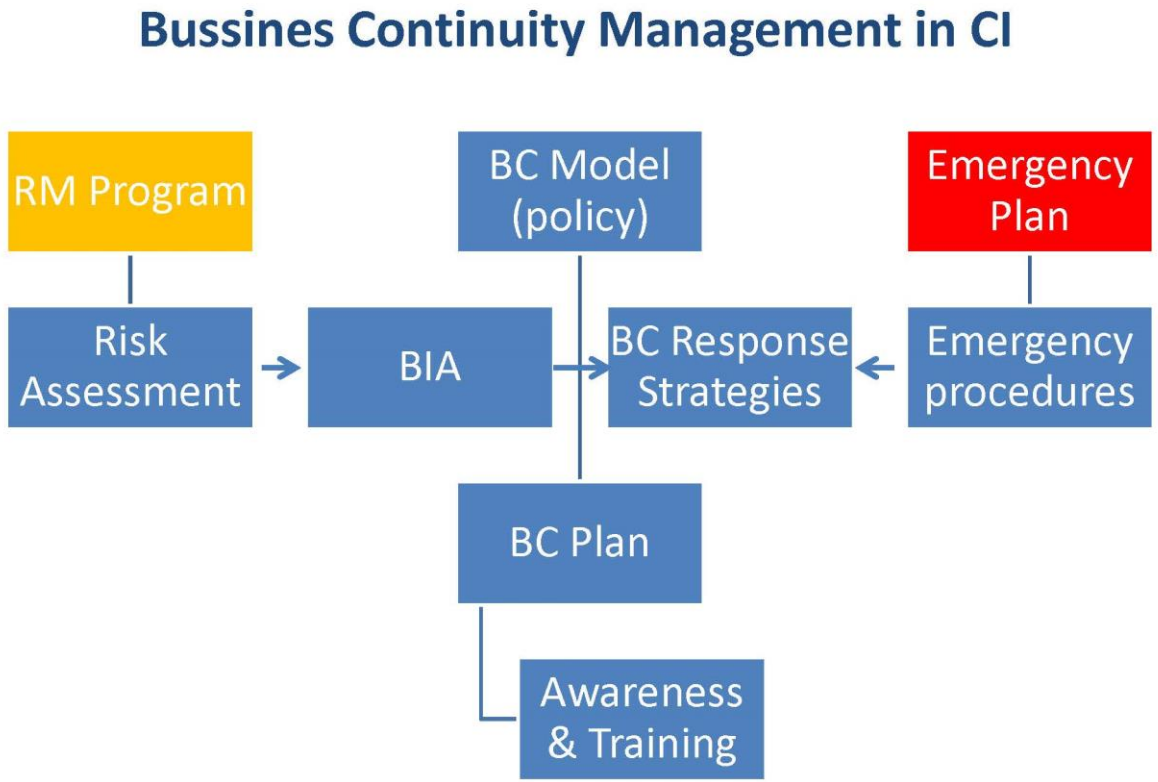
PESI: modelo integrado de Gestión de Riesgos hacia la Continuidad de Negocio y Resiliencia

Integración de Modelos y Técnicas de evaluación y gestión de Riesgos (Crisis, Emergencias) y Continuidad de Negocio (Resiliencia)

El **Negocio** es: producir energía, vehículos, hidrocarburos, agua potable, transportar viajeros y mercancías,…

¿cómo integrar los Modelos preventivos de Seguridad y Ciberseguridad?
¿Y en las Cadenas de Valor industrial (proveedores, subcontratación, cadenas logísticas?

AMPLIAR EL MODELO DE SEGURIDAD INTEGRAL A LA CADENA DE VALOR



Elementos en la Gestión de Riesgos (en proyectos e I+D)

1. **Metodologías AR (Análisis y Evaluación de Riesgos)**
   1. Identificación de Amenazas y Riesgos
   2. Valoración de la posible afección (elementos afectados y grado)
   3. Efectos en cascada (dependencias internas y externas)
2. **Sistemas de Detección y Alerta temprana**
3. **Medidas de Remediación**
   1. Evitar Riesgos (Seguridad desde el Diseño): no sólo desde la transformación digital
   2. Plan: mejoras en Elementos (instalaciones) y Procesos (incrementar la Resiliencia)
   3. Contratos de Seguros
4. **Colaboración Público-Privada en Crisis y Emergencias**
   1. Protocolos (plan interno) de Gestión de Crisis: plan de Autoprotección
   2. Protocolos de colaboración con Equipos de Emergencias (Protección Civil)
   3. Plan de Comunicación a la Sociedad

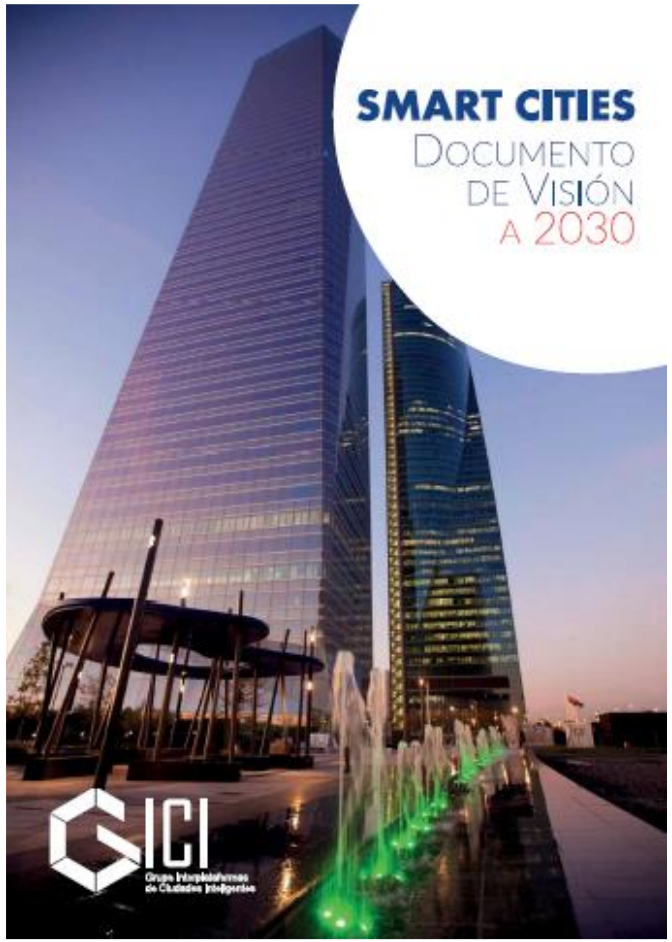
Tipologías de Riesgos (gestión integral)

- **Riesgos (tecnológicos) industriales /Infraestr.**: propios del sector/procesos (técnicas AR conocidos)
  - Seguridad y fiabilidad desde el diseño (procesos)
  - Seguridad y salud estructural (BIM y seguridad)
  - **Factor Humano (cultura de seguridad)**
- **Riesgos Laborales**: Seguridad y Salud en el Trabajo (PRL)
- **Riesgos Medioambientales**
  - Desastres naturales (terremotos, lluvias/inundaciones, vientos/huracanes…): instalaciones, movilidad, RR
  - Efectos del Cambio Climático (nivel del mar, olas de calor, sequías…)
  - Accidentes naturales/provocados: incendios, escapes…
- **Riesgos en la Movilidad** y cadenas logísticas
  - Accidentes viales (personal interno y subcontratado): in-itinere y en misión
  - No disponibilidad Redes de Transporte (terrestre, ferroviario…): Riesgos en Infraestructuras y Med-Amb.
- **Riesgos de carácter Socio-económico o político** (países inestables, conflictos, falta RR)
- **Riesgos en las Cadenas de Valor** (cadenas industriales y suministro) y Zonas Industriales
- **Riesgos de Seguridad** (Security, delincuencia y ataques deliberados)
  - Físicos (sabotajes –personal interno- y ataques)
  - Lógicos (ciberseguridad: SI y/o industriales ICS)

PESI 2030 vision on the Smart & Resilient City

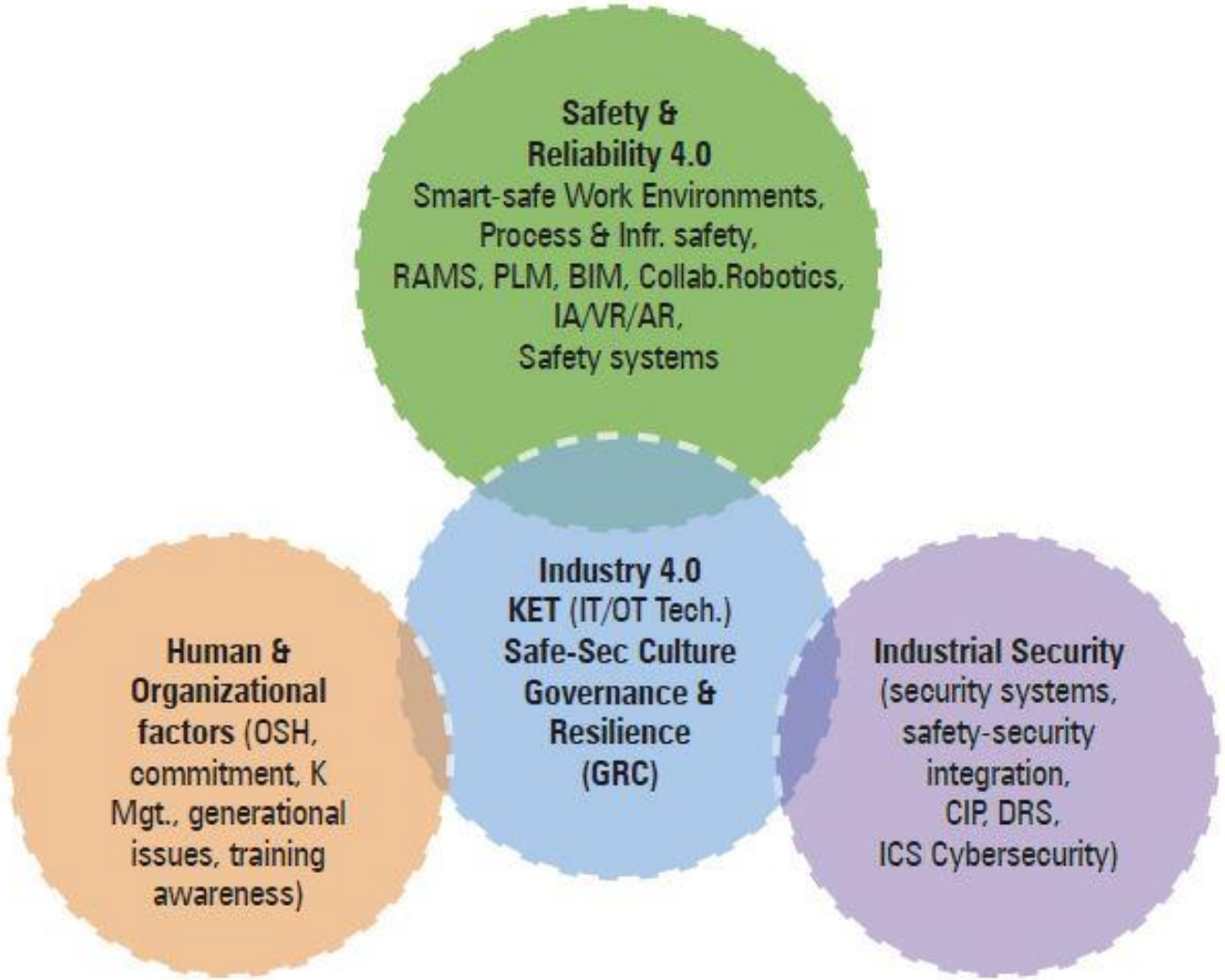
Concept of Secure Society could be very broad from different perspectives *(safety, security, cybersecurity) or* focus (resilience, protection, emergencies, reliability, industrial, road safety, Health, wellbeing…). ETPIS and PESI have faced future challenges for the Smart and Secure Safety & Communities through four **main pillar**:

1. A **Governance model for integral risk management and resilience** of the essential services (CI Operators) for citizens,
2. **Reliability** of Utility networks and urban infrastructures and installations,
3. **Security and protection of citizens, Infrastructures and heritage of the City**
4. And the **cyber-security of control systems in the City** (utilities networks, urban systems and infraestructures related to essential services).



Europea Comisión (2021): foco en la Persona -> Industria 5.0

PESI / ETPIS: Innovation circles for EU Horizon Europe



Agenda Estratégica de Innovación y Desarrollo tecnológico y Retos Sociales: Seguridad, Salud laboral y Sociedades Seguras

Grupos de Trabajo:

- **Cultura Preventiva, Salud y Bienestar Laboral (factor humano/organiz.)**
  - Estrategias PRL/factor generacional. Riesgos psicosociales. Adicciones digital
  - Tecnologías para Información/formación (RV/RA; IA). Digitalización PRL/SST
- **Seguridad y fiabilidad Industrial (GT-Safety)**
  - Entornos inteligentes y seguros de trabajo: EPIS, Wearables, sist. seguridad
  - Industria conectada/4.0-5.0 (IoT, CoRobot, BigData, IA, RV/RA, Drones…)
  - Seguridad de Infraestructuras (BIM + Safety)
- **GI Movilidad Segura**
  - Seguridad Vial Laboral, Movilidad Segura y sostenible (Marco de Referencia en MGA)
  - Transporte seguro (Mercancías peligrosas, Transp. público)
- **Seguridad corporativa, Gobernanza y Resiliencia (GT-Security)**
  - protección de infraestructuras críticas (**factor humano en Seguridad**),
  - **Resiliencia** y continuidad del servicio, Ciberseguridad
- **G.I. ciber-seguridad (industrial) con PTE-Disruptive**
- **G. Inter-Plataformas (Ciudad Inteligente, Economía Circular…)**

PROGRAMA MARCO EUROPEO Innovación e I+D
Horizonte Europa: Pilar II Retos Sociales

Los **objetivos** específicos del **Pilar II de Horizonte Europa** son:

- generar conocimiento, intensificar la repercusión de la investigación y la innovación (I+I) en la elaboración y aplicación de las políticas de la Unión, así como en el apoyo a estas políticas,
- y favorecer el acceso y la adopción de soluciones innovadoras en la industria europea, en especial en las pymes, y en la sociedad,
- para hacer frente a los desafíos mundiales, incluido el **cambio climático y los Objetivos de Desarrollo Sostenible (ODS**).

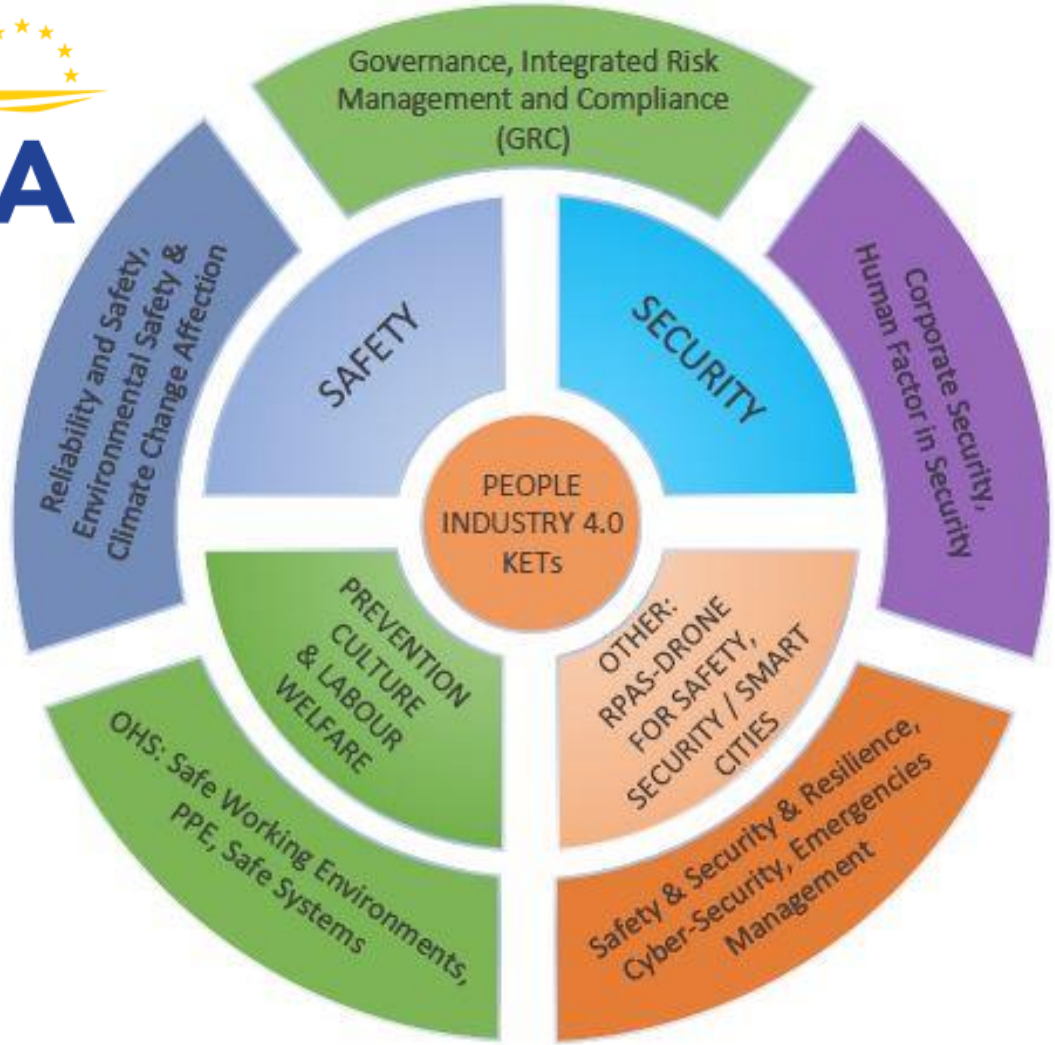
Las actividades de I+I se llevarán a cabo en los siguientes clústeres:

1. **Salud (entornos saludables de trabajo)**
2. **Cultura, creatividad y sociedad inclusiva**
3. **Seguridad civil para la sociedad: PIC, DRS y Ciber-Seguridad (Resiliencia)**
4. **Mundo digital, industria y espacio; (SWE)**
5. **Clima, energía y movilidad;**
6. **Recursos alimentarios, bioeconomía, r. naturales, agricultura y medioambiente**

- **Nota: la aplicación de la IA está contemplada en todos los CL**

PESI: Grupos de Trabajo asociados a la Visión y Retos Sociales (Unión Europea, UN-ODS)

HORIZONTE EUROPA



Ámbitos de Seguridad Corporativa y Protección de Infraestructuras (industriales, servicios esenciales a la Sociedad y Ciudad)

Security y PIC, Operación, Ciberseguridad y Resiliencia, Directivas Europeas Seguridad-Ciber; I+D+I: HORIZONTE EUROPA Cluster-3

Marco de la Seguridad Corporativa en Infraestructuras Críticas (España): Estrategias Nacionales de Seguridad, Ciberseguridad y Ley PIC

Despliegue Ley PIC (CNPIC, trasposición a Dirª Resiliencia):

- Sectores e Infraestructuras Críticas y Servicios esenciales:
  - Operatores Privados (tipo industrial 2/3 de las ICs)
  - Administración Pública
- Sectores: Estudios sectoriales (8 de 13 sistemas industriales)
- PSO Plan de Seguridad del Operador
- PPE Plan de Protección Específico (instalaciones individuales)
- Plans y Organización de la Seguridad Corporativa
  - Estrategia y Gestión Riesgos integral (Safety-Security-Cyber)
  - Certificación de los Planes y sistemas (CNPIC)
- Ciberseguridad: ISO-2700x/ENS, ahora NIS2 (y Ciber-Resiliencia)

+ Nueva Ley de Seguridad Privada (gestionada: servicios de seguridad física y **Ciberseguridad** subcontrados: SOC…)

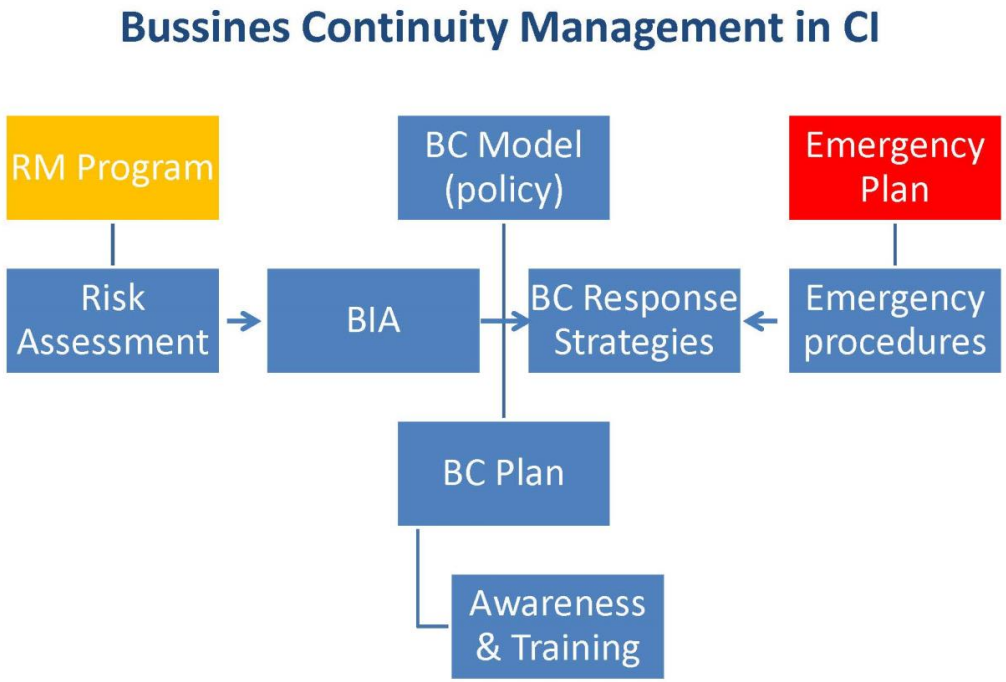
Systems and Technology towards Resilience

- Organization and new responsabilities in Safety & Security
  - **Integrated Risk Analysis** & Business Intelligence (TS/CI, new risks: conflicts and radicalization)
    - Operational Reliability and Safety (engineering / process): industrial and environmental Safety and OSH
    - Security-Cybersec of industrial installations, infrastructures and networks
    - Information Security (IT-OT: Cybersecurity)
  - **GRC Strategy** &organization based on a real **SECURITY-SAFETY integration**
- New Framework (**CIP/NIS2 Directive** & National Laws, EU Goals and Resilience, Horizon Europe-Cluster3/Security):
  - **Convergence safety- security** (from different visions: industrial safety, cybersecurity and corporate security): integrated **Risk Mgt./Dependencies**
  - **DRS** (**Natural Disasters Resilience, including climate change**) and Tech. Accidents (Civil Protection and emergencies plans): **Crisis Mgt.**
  - Critical Infrastructures **Protection** (industry / utilities/ transport…) towards **BC**
  - **Cybersecurity** by design (IS security, automation&control systems/SCADA)
  - **Business (essential services) Continuity and Resilience**

PESI: modelo integrado de Gestión de Riesgos hacia la Continuidad de Negocio y Resiliencia

Integración de Modelos y Técnicas de evaluación y gestión de Riesgos y de Emergencias y Continuidad de Negocio (Resiliencia):

¿cómo integrar los Modelos Preventivos de Ciberseguridad? ¿Y en las Cadenas de Valor Industrial, subcontratación, cadenas industriales/logísticas?



RA and BIA (Dependencies assesment)

- **Risk and Dependencies Assesment:**
  - **Functions and Services** evaluation (***criticity*** *level*)
  - **Resources** (requirements):
    - Personnel
    - Equipment
    - Systems (SW, ITC) and **Cybersecurity**
    - Utilities (Inter-dependencies)
    - Materials …
- **Business Impact Analysis:**
  - Intra-dependencies
  - Inter-dependencies (external CIs)
  - Cascading effects (up-stream & down-stream)

Modelo Criticidad (evaluación, 10 categorías) y Dependencias

Categories	Critical Elements of the CI	INTRA-DEPENDENCIES	Direct Impacts	Control Rooms (Operation)	Security Control Rooms	Info Systems (OT/IT, ciber) &Comm	Staff - Mgnt Board & Crisis Committee	Essential Teams	other staff & ext personnel	Critical Proc-1	Critical Proc-2	Critical Proc-n	Security Equipment & Systems	(essential) Equipment & appliances	Infraestructures (buildings)	External Services &Supplies	Others
I	Control Rooms (Operation, Security, Integral)			■													
I	- Security Control Rooms				■												
II	Information Systems (OT/IT, ciberseg.) &Communications (voice, radio, IP...)																
III	Staff - Mgnt Board & Crisis Committee																
III	- essential Teams (Op&Maint, Emerg, ITC)																
III	- other personnel & subcontractors																
IV	Critical Processes (industrial/essential service, restricted areas...; safety systems)									■							
IV	Critical Process-2										■						
IV	Critical Process-n											■					
V	Security Equipment & Systems																
VI	Equipment & appliances (esential)																
VII	Infraestructure (buildings, installations)																
VIII	External Services &Supplies (Subcontr&Providers)																
IX-X	Others (economic, legal, Soc accept., specific)																

Intra/Inter-dependencias de los Elementos/sistemas críticos (elementos críticos: CIBERSEGUROS # Dirª Ciber-Resiliencia: Certificación!!)

	INTER-DEPENDENCIES	Direct Impacts	Energy	Gas/oil	Water	Telecoms (voice, data &ISP)	Location & Environment	Transport Infrast. (road, train	Logistics (& purveyance)	Security, Civil Protection & Emergencies	Others
Categories	Critical Elements of the CI										
I	Control Rooms (Operation, Security, Integral)					5					
I	- Security Control Rooms					5					
II	Information Systems (OT/IT, ciberseg.) &Communications (voice, radio, IP...)					5					
III	Staff - Crisis Committee										
III	- essential teams (Op&Maint, Emerg, ITC)							4			
III	- other personnel & subcontractors										
IV	Critical Processes (industrial/essential service, restricted areas...; design, organization, tasks, safety systems)										
IV	Critical Process-2								4		
IV	Critical Process-n										
V	Security Equipment & Systems										
VI	Equipment & appliances (esential)										
VII	Infraestructure (buildings, installations)						2	2			
VIII	External Services &Supplies (Subcontr&Providers)										
IX	*Economic & Legal (Stability); Societal acceptance*										
X	Others (specific in the CI)										

Ámbitos de Ciberseguridad


AI Security


Cybersecurity Culture


DevSecOps


Extended Detection and response (XDR)


Hacking


Incident Response


Leadership


OT Security


SASE - Secure access service edge


Threat Intelligence


Zero Trust

Cybersecurity in European Union: webs, Directives and Acts

1. The NIS 2 Directive	
2. The **European Cyber Resilience Act** (en desarrollo, 2024?: previsible aplazamiento)	9. The European Data Act
3. The Digital Operational Resilience Act (**DORA**)	10. European Data Governance Act (DGA)
4. The **Critical Entities Resilience Directive** (**CER**)	11. The Artificial Intelligence Act
5. The Digital Services Act (DSA)	12. The European ePrivacy Regulation
6. The Digital Markets Act (DMA)	13. The European Cyber Defence Policy
7. The European Health Data Space (EHDS)	14. The Strategic Compass of the European Union
8. The European Chips Act	15. The EU Cyber Diplomacy Toolbox

HORIZON EUROPE – Cluster 3 Civil Security for Society 2023 call (R&D topics)

Opening: 29 Jun 2023. Deadline(s): 23 Nov 2023

Destination - Resilient Infrastructure

INFRA-01: Improved preparedness and response for large-scale disruptions of European infrastructures

- HORIZON-CL3-2023-INFRA-01-01: Facilitating strategic cooperation to ensure the provision of essential services (IA, 1 Pr, 4,5 M€)
- HORIZON-CL3-2023-INFRA-01-02: Supporting operators against cyber and non-cyber threats to reinforce the resilience of critical infrastructures (IA, 2 Projects, 4,5 M€)
- HORIZON-CL3-2024-INFRA-01-01: Open Topic (5M€)

INFRA02 – Resilient and secure urban areas and smart cities

- HORIZON-CL3-2024-INFRA-01-02: Resilient and secure urban planning and new tools for EU territorial entities
- HORIZON-CL3-2024-INFRA-01-03: Advanced real-time data analysis used for infrastructure resilience

Destination - Increased Cybersecurity:

- CS01 - Systems Security and Security Lifetime Management, Secure Platforms, Digital Infrastructures
- CS02 – Privacy-preserving and identity technologies
- CS03 - Secured disruptive technologies

Horizonte Europa, Cluster 3: topics previos INFRA

Addressing interdependencies and systemic risks

Besides the classical approach of protecting infrastructures by sector, a stronger focus on the systemic dimension of attacks is necessary. As such, not only **interdependencies** within one type of infrastructure (or closely related types) can be taken into account, but **large scale disruptions** also with a view of the specific challenges of the cross-border dimension. Specific attention could be dedicated to **Hybrid Threat scenarios**.

- Large-scale Vulnerability Assessments and risks management capabilities, forecasting of emerging risks (via AI)
- Simulations to prepare for systemic disruption of several key infrastructures
- Cross-border scenarios (also with third-countries)
- Better anticipation of systemic risks (including advanced FDI-screening, technological risk assessment)
- Societal resilience against CI-disruption with **Hybrid Attacks** and false news (e.g. finance infrastructure, food-supply and medical system)

Increasing protection and resilience of Critical Infrastructures

Research on CIP is a well-established domain with significant results achieved. Due to the fast evolving technological landscape there are however constantly new challenges and opportunities. **Resilience and Preparedness are keywords to possibly define upcoming research priorities of a cross-cutting nature.**

Example of INFRA R&D proposal: systemic approach (SecureChem: CIP and Dependencies on Chemistry)

Geographical data
Weather
Flood
Energy mix
Transport
Food
Gas network
Seismicity
Heath
Land use & urban planning
Sensitive sites
Ground and underground data
Water systems

existing data bases and periodic reports

CIDER
Critical Infrastructure Disruption Exploration Room

New systems to collect data

Risk & data management

Simulation modules to assess in detail all aspects of interdependent physical, cyber threats and incidents, and the cascading risks resulting

Collect data for prevention, detection, response and mitigation of combined physical and cyber threats to critical

Multi-risk assessment at territory level

Procedures & accident response scenarios at territory level

Steering evidence-based system

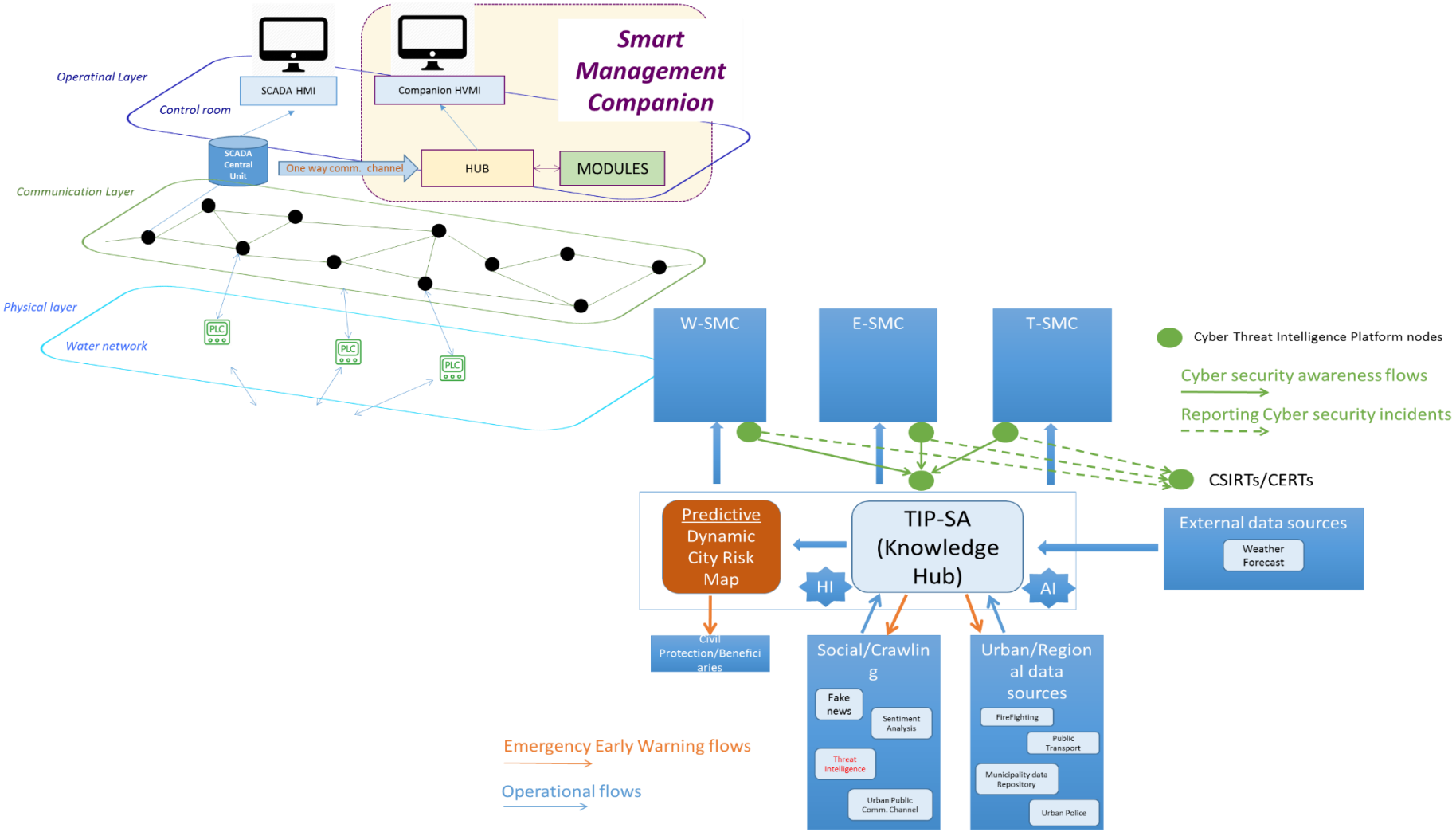
Requirements and recommendations for policy planning, engagement of the civil society, and investment measures

Virtual control room to provide and share a common picture

Geographic information system (GIS) and visual digital system

(decision, coordination, communication)

Example of INFRA R&D proposal: systemic approach (TAU: energy/water systems and Cities)



HORIZON EUROPE – Cluster 3 Civil Security for Society 2023 call (R&D topics)

Destination - Disaster-Resilient Society for Europe: "Losses from natural, accidental and human-made disasters are reduced through enhanced disaster risk reduction based on preventive actions, better societal preparedness and resilience and improved disaster risk management in a systemic way." Safeguarding and securing society, including adapting to climate change (Response, Awareness/Civil protection, Communication Systems, Bio threats, CBRN cluster)

DRS01 - Societal Resilience: Increased risk Awareness and preparedness of citizens, topic(RIA, 2 pr., 4M€):

- **HORIZON-CL3-2023-DRS-01-01: Improving social and societal preparedness for disaster response and health emergencies**

DRS02 - Improved Disaster Risk Management and Governance, topic(RIA, 1 pr., 4M€):

- **HORIZON-CL3-2023-DRS-01-02: Design of crisis prevention and preparedness actions in case of digital breakdown (internet, electricity etc.) – tipo INFRA-**

DRS03 - Improved harmonisation and/or standardisation in the area of crisis management and CBRN-E, topic(s):

- **HORIZON-CL3-2023-DRS-01-03: Operability and standardisation in response to biological toxin incidents** (RIA, 1 pr., 6M€)
- **HORIZON-CL3-2023-DRS-01-04: Internationally coordinated networking of training centres for the validation and testing of CBRN-E tools and technologies in case of incidents, with consideration of human factors** (IA, 1 pr., 4 M€)

DRS04 - Strengthened capacities of first and second responders, topic(s):

- **HORIZON-CL3-2023-DRS-01-05: Robotics: Autonomous or semi-autonomous UGV systems to supplement skills for use in hazardous environments** (RIA, 2 pr., 4 M€)
- **HORIZON-CL3-2023-DRS-01-06: Increased technology solutions, institutional coordination and decision-support systems for first responders of last-kilometer emergency service delivery** (RIA, 1 pr., 3,5 M€)

RESISTAND (the Performance Reference Model): a Disaster Management organization

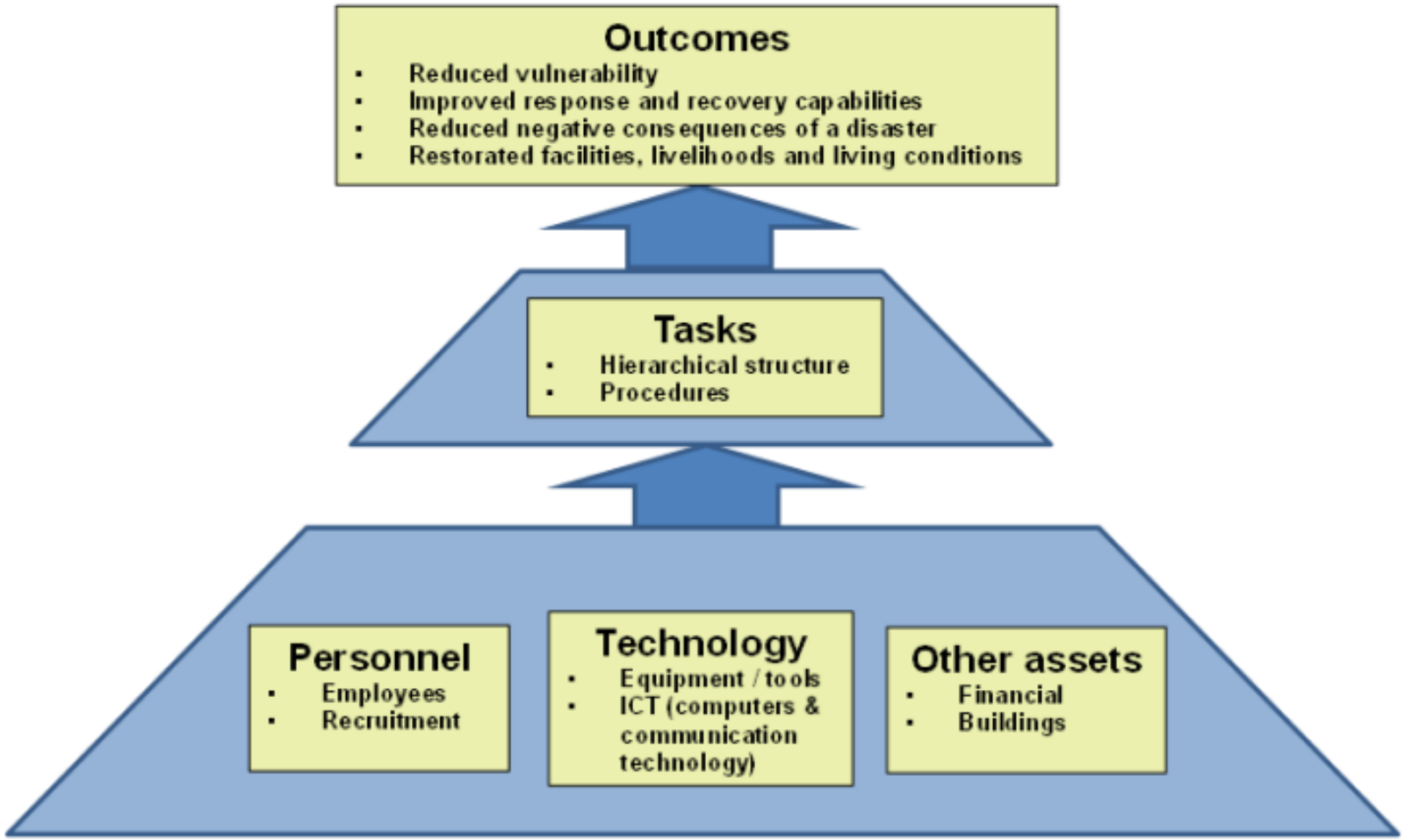


Figure 6: Model of a disaster management organisation

RESISTAND (H2020-DRS): Resilience & Crisis Mgt Framew.

Figure 1: Disaster Management Cycle

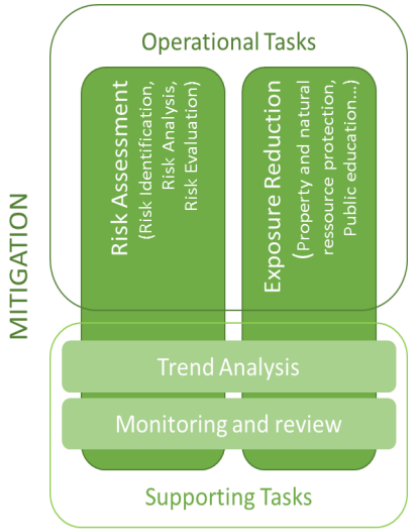


Figure 2: Mitigation Tasks of RCF

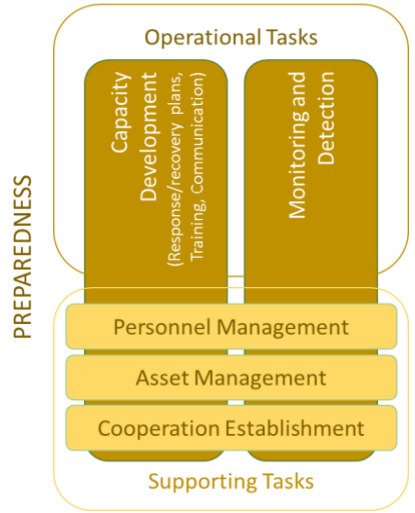


Figure 3: Preparedness Tasks in RCF

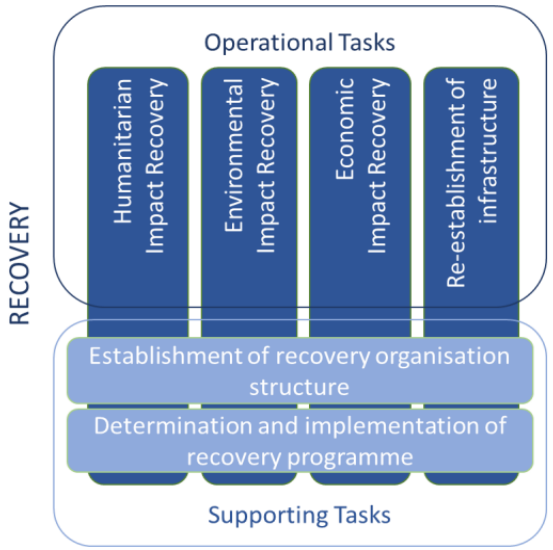


Figure 5: Recovery Tasks in RCF

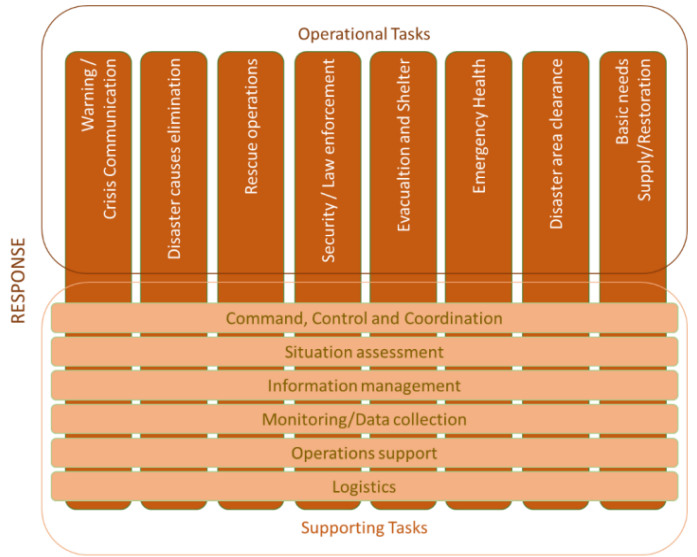


Figure 4: Response Tasks in RCF

Final recommendations

CI Operators cooperation & Resilient Cities

Inter-dependencies: cooperation between CI Operators

- **CI Operators: Security and Resilience Plans**
  developed evaluating the main and direct **dependencies** and considering other "theoretical inter-dependencies" (defined by the strategic sectoral security plans coordinated by Governments and Operators)
  - Enlarge depedencies Assesment, based on an in-detail analysis for all active elements in the CI network/system (previous experiencies…)
  - Security Plans and related information "classified" or "restricted"
  - Difficulties for sharing relevant information
- Build ***spaces for confidence***: e.g. CERT and Technical Committees (led by National Agency for CIP) for CI Operators Security Dpts.
- Resilience **Exercices** (CI Operators in collaboration) **and Cyber-exercices**

Urban Resilience and Safe CI Operators

- **Community** requirements for availability and *resilience of the essential services* (CI) at Local and Regional levels
- Public **contracts** (concessions) for Utilities and other public services operated by private companies: include clauses for *QoS and "resilience" plans to the Operators*
- New **collaboration** schemes between CI Operators and Municipalities and Regional Governments (PPP for Security and Resilience)

Moitas grazas. Muchas gracias
¿Preguntas y comentarios ?

J. Javier Larrañeta, Secretario General
javier.larraneta@tecnalia.com
secretario-tecnico@pesi-seguridadindustrial.org

XV Aniversario

PLATAFORMA TECNOLÓGICA ESPAÑOLA DE SEGURIDAD INDUSTRIAL

SECURITY DEFENSE SEDEXPO EMERGENCY

GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA E INNOVACIÓN

AGENCIA ESTATAL DE INVESTIGACIÓN

MINISTERIO DE CIENCIA E INNOVACIÓN CDTI

@CDTIoficial