European Technology Platform on
Industrial Safety
Safety for Sustainable European Industry Growth

PLATAFORMA TECNOLÓGICA ESPAÑOLA DE SEGURIDAD INDUSTRIAL

ETPIS-PESI (cross ETP initiative on Industrial Safety and Security towards Resilient Organizations, Infrastructures and Communities)

(Production plants, Utility and Transport networks and critical services for the Smart City)

EU-OSHA Campaign: best practices workshops

(Brussels, 6 March 2019)

Javier LARRAÑETA
PESI Secretario General
ETPIS Executive Board

tecnalia Inspiring Business

Indice

- **ETPIS PESI:** European & Spanish Technology Platforms (2002) on **integral Industrial Safety**
  - Integral Vision Governance, RisK Mgt. for the Resilience (Industry, Networks & Infrastructures)
  - Safe &Secure Cities (under CIP: protection of Industrial & Transport Critical Infrastructures)

- **Deployment areas: Safety, OSH, Reliable Operation, Security and Ciberseguridad**

- **Industrial Safety in ETPIS 2 (SafeFuture for H2030)**
  - Safe-Infrastructures and Resilience

- **Security, Resiience and Critical Infrastructures Protection (Secure Communities)**
  - Technologial priorities in Industriy, Networks and relevant Infrastrcutures

European Technology Platform on
Industrial Safety
Safety for Sustainable European Industry Growth

PLATAFORMA TECNOLÓGICA ESPAÑOLA
DE SEGURIDAD INDUSTRIAL

ETPIS & PESI: Technology Platforms on (integral) Industrial Safety & Security

ETPIS- PESI 2020 Vision

« Innovation and technology development (R&D+i) based on a global and integrating vision on Industrial Safety and Risk management»

(Safety + Security)

Deployment areas:

- **Safety (processes, instalations)**
- **Occupational Safety & Health**
- **Environmental Safety (SHE)**
- **Corporate Security and Resilience** based on the CIP European Directive **(plants, transport infrastructures & utility networks)**

1.- Industry (Corps & SME, Associations)

- △ Enterprises and Industrial Corporations (many sectors)
- △ Technology-based SME, Engineering & Consultancy firms)
- △ Associations (Manufacturing, Energy, Security, PPE, Fire, etc)

2.- Government: Ministeries & Regional Bodies

- △ Ministry of Science, Innovation & Universities: AEI, CDTI
- △ Ministry of Industry: Industrial Safety, Connected Industry 4.0
- △ Min. Economy: Digital Development (INCIBE Cybersecurity)
- △ Ministry of Employment (OSH): INSST
- △ Ministry of Public Infrastructures (Transport Inf, Haz.Goods…)
- △ Ministry of Ecological Transition: Environment
- △ Ministry of Interior (DG PCyE, CNPIC, DG-Traffic)
- △ Public Bodies in Autonomous Governments

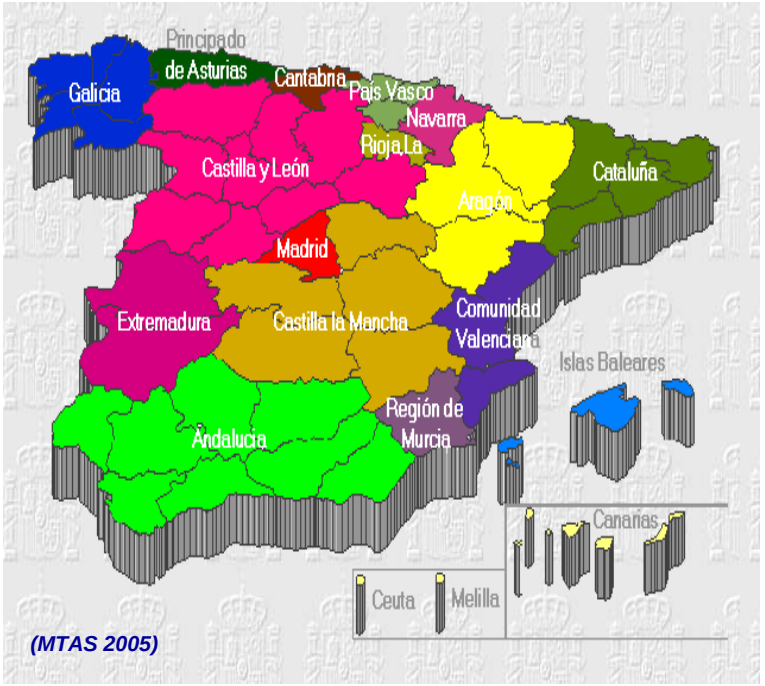
3.- Academia and Research Institutions & Labs

- △ Research Institutes, Labs, Technology Centres
- △ R&D units at Universitiess

4.- Other relevant institutions

- △ Asociación Española de Normalización (AENOR)
- △ Insurance, Prevention & Medical services: accidents at work, professional disseases

PESI partners



60 Founding Members
(PESI: non-profit Association)

Around 850 active Organizations
+2500 technicians members

H2020: Industrial Leadership (NMBP) and Societal Challenges (Secure Societies)

Adaptation of PESI Focused Groups to HORIZON-2020 *(since 2013)*

- **Industrial Safety** (Smart Working Environmets, Structural Safety & ageing infraestructures –industrial plants, transport infrastructures & utility networks-)
- **Human & Organizational Factors** (safety culture, Road Safety at Work,…)
- **Corporate Security** (CIP, resilience, business continuity and ciber-sec)
- **Inter-Platforms Groups: Nanosafety, Digitalization, COROBOT, RPAS/Drones**
- **IPG on Smart & Resilient City** (Safety/Security/Cyber, Crisis Mgt., Disasters & Climate Change, Mobility, Circular Economy…)

HORIZON-2020	INDUSTRIAL LEADERSHIP						SOCIETAL CHALLENGES					
ETPIS (PESI): New Focussed Groups	ITC	NANO	BIO	MAT	PROD	SPACE	HEALTH	FOOD	ENERGY	TRANSP	CLIMATE	SEC-SOC
SafeFuture		X			X			X	X	X	X	X
ERANET (SAF€RA)					X							
Safe-Production (&Safety Products)		X			X				X			X
Safe-Energy									X	X		X
Safe-Infrastructures					X				X	X	X	X
Safety Transport (haz. goods)										X		X
Security: convergence with Safety (& CIP - Infrastructures Protection-)												X
- Emergencies	X				X	X				X	X	X
- Cibersecurity	X								X	X		X
Nanosafety & Nano-toxicology (Joint ETP Group)		X	X	X	X		X	X				X
Environmental Safety		X	X	X	X	X		X	X	X	X	X
Miscellaneus												
- Ageing at Work (Healthy & Active Ageing)	X				X		X					
- Road Safety (at work)										X		X
- Prevention Culture & Training					X							X

PESI (ETPIS): FGs for H2020 since 2018 (X Aniversary)

- **SAFETY**
  - **INDUSTRIAL SAFETY** (Smart working environments & Factory 4.0): PPEs, Safety products & systems, Sensoring-Monitoring, NDT, RAMS & Assets Management including Ageing)
  - **Structural Safety** (Safe-Infrastructures, in coord. with **Construction & Transport ETPs**)
  - **Emergencies Management** (joint with FG-Security)
  - **Civil use of RPAS-drones on Safety-Maintenance & Security** (joint with FG-Sec)

- **SECURITY** (inc. Industrial Cybersecurity)
  - **Governance, Resilience & CIP: Safety-Security Integration (ETPIS)**
  - **Technologies for Security; People & Assets Protection**
  - **Industrial CIBERSECURITY**

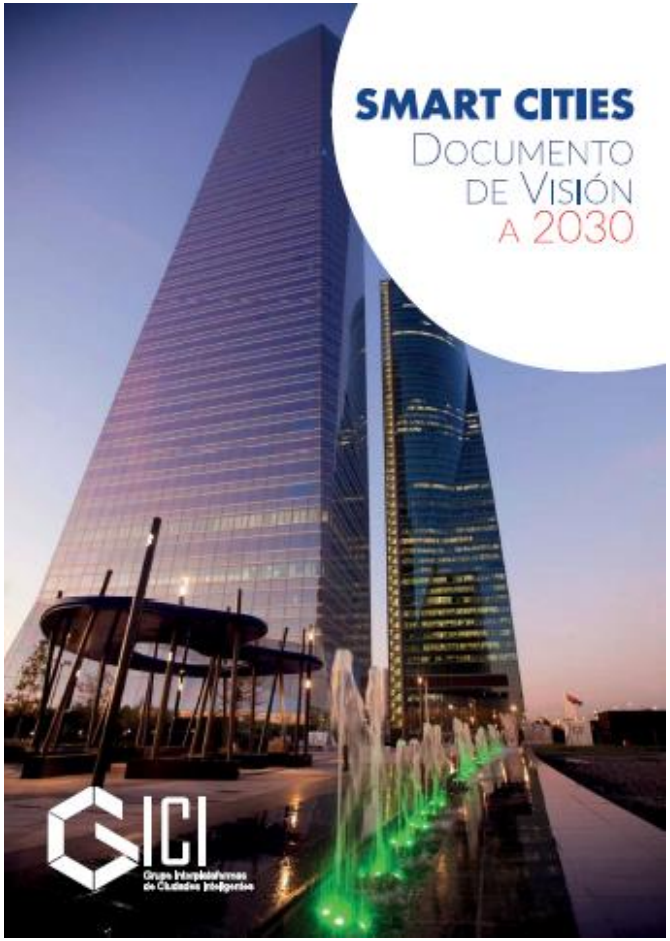
- **HUMAN & ORGANIZATIONAL issues**
  - **Safety Culture, Health & wellbeing** (Ageing/generational issue, Drugs at work…)
  - **Road Safety at Work**
  - **Human factor in Security & CIP** (Insider threats)

- **Inter-Platforms Groups:**
  - **GICI Smart & Resilient Cities:**
  - **SAFE MOBILITY** (new from Autum 2018): Paradigm, Tech. for Safe Mobility, ITS, Secure Transport, Hazardous goods transortation

PESI 2030 vision on the Smart & Resilient City

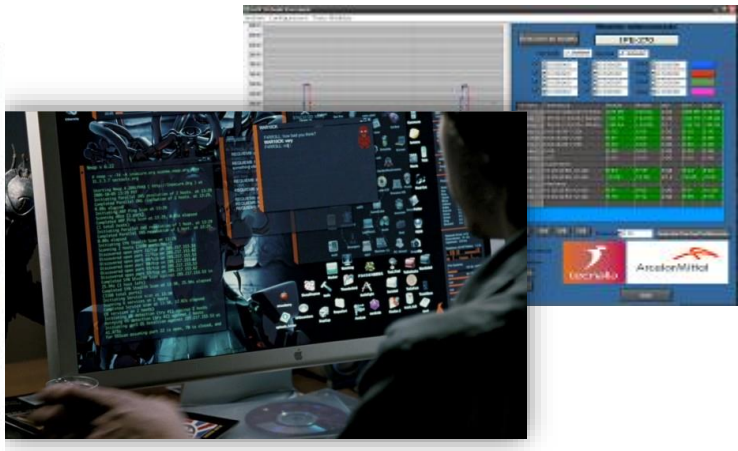
Concept of Secure Society could be very broad from different perspectives *(safety, security, cybersecurity) or* focus (resilience, protection, emergencies, reliability, industrial, road safety, Health, wellbeing…). ETPIS and PESI have fase future challenges for the Smart and Secure Safety & Communities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



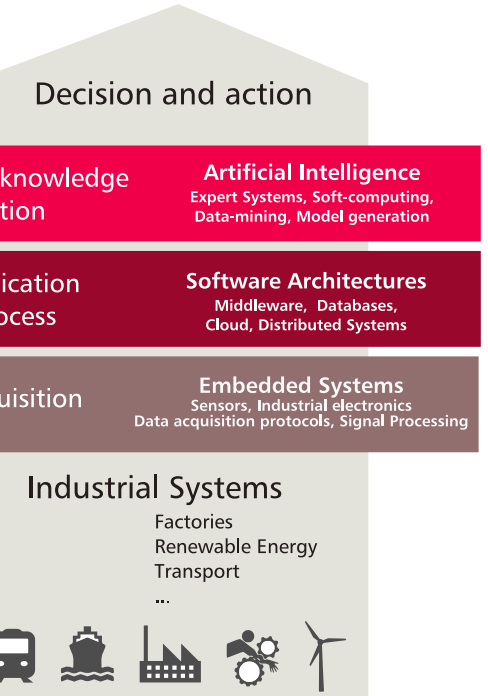
Safe-Infrastructures: vision

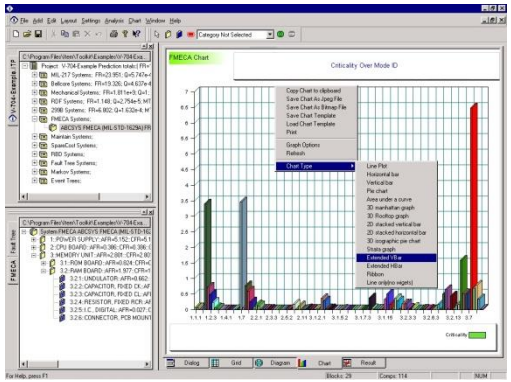
- SafeFuture / Safe-Infrastructures vision:
  Safety-Reliability-Resilience
  - Research towards new concepts and systems, with Safety & Reliability as essential elements in Industrial plants and Utilities networks
  - Industrial infrastructures: similar technology & organizational challenges related to ageing >>> common research objetives for safety & reliability
  - **Industrial Control Systems: also ageing , IT/OT evolution + cyber-security threats !!**



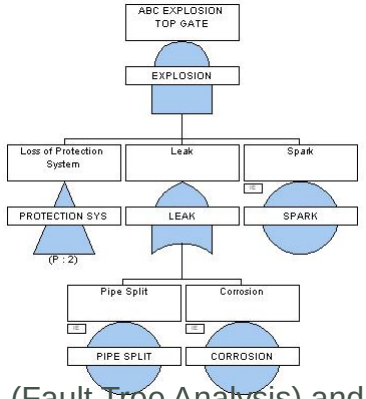
Safety-Security (operation & maintenance)

- **RAMS** (Reliability, Availability, Maintenance & Safety **+Security**) as the reference model
  - **Analysis, Evaluation and Risk Mgt.** (for the whole life-cycle)
  - Predictive Models for maintenance (based on situation: diagnosis, prognosis)
  - Learning from behaviour (artificial intelligence). **Digital Tweens**.
  - Monitoring integrated Systems
  - Life-Cycle and **Ageing** Management
  - **ICS Cybersecurity**
  - **INFORMATION SYSTEMS evolution: IoT, Big-Data, Cloud comp., Cyber-physical Syst. !!**

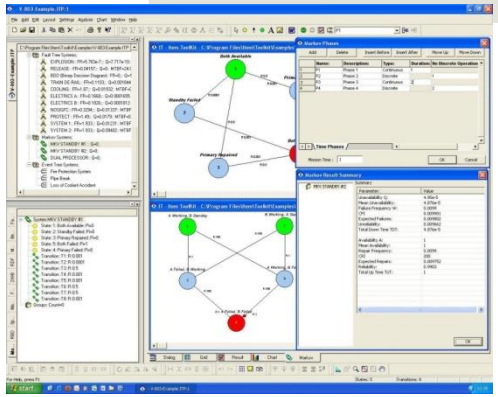




FMECA (Failure Mode, Effects and Criticality Analysis)



FTA (Fault Tree Analysis) and ETA (Event Tree Analysis)



Behaviour modelisation (Markov nets, Altarica,etc…)

New Governance and integrated Risk Management model (reliability, safety, security and resilience under Industry 4.0 paradigm)

Governance, Integrated Risk Mgt. and Compliance (GRC)

Process & Infrastructures Mgt.: Reliability and Safety (Operation, RAMS, PLM, Maintenance, BIM)

Environmental Safety & Climate change afection

Emergencies Mgt. (Disaster/Crisis Preparation, Civil Protection collaboration)

Safety-Security & Resilience Plans (business continuity, CI dependenc. indicators,…)

Cyber-Security (Industrial Information Systems)

Corporate Security (protection of staff, infrastructures and K./IP…)

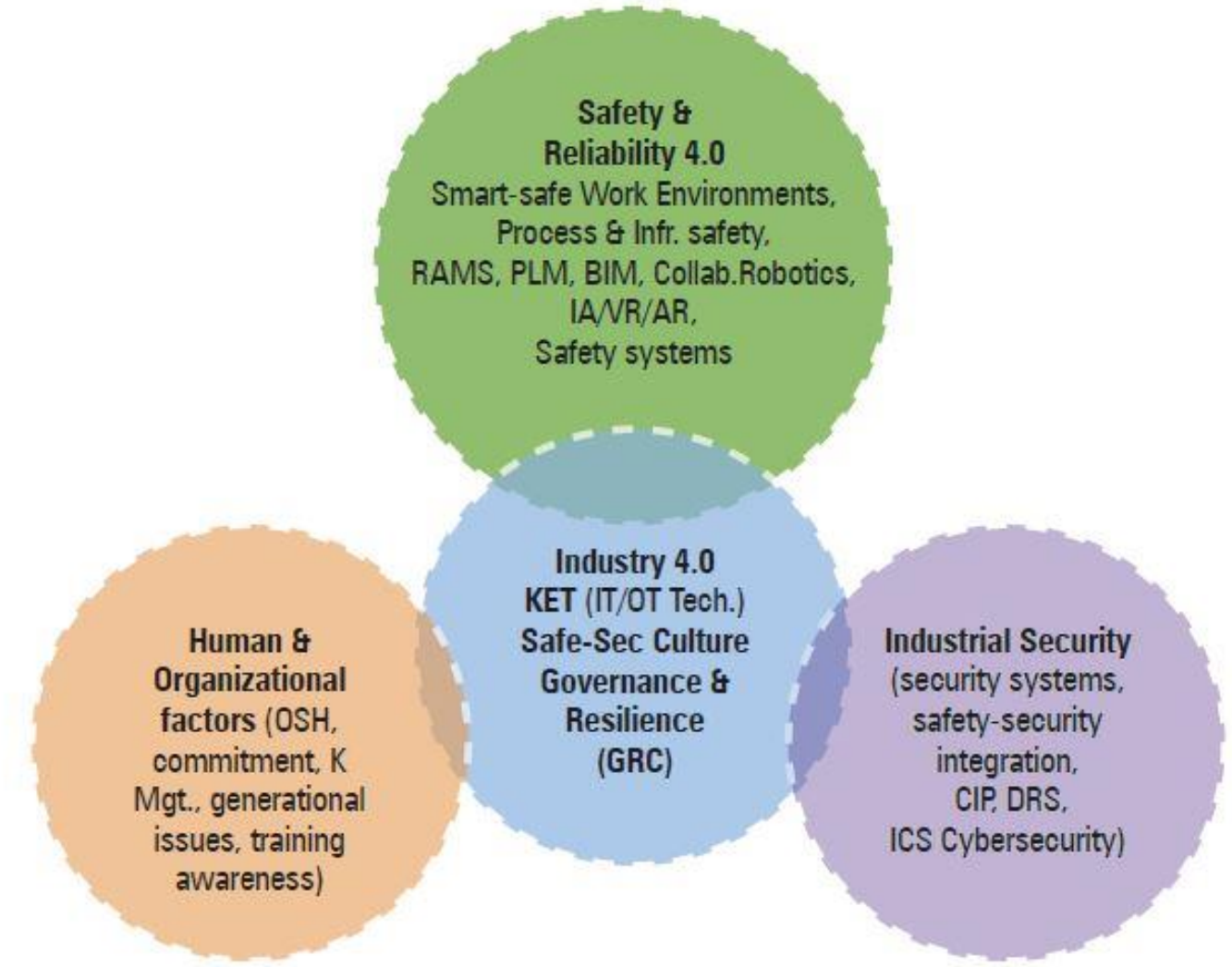
Human Factor in Security (Personnel Security)

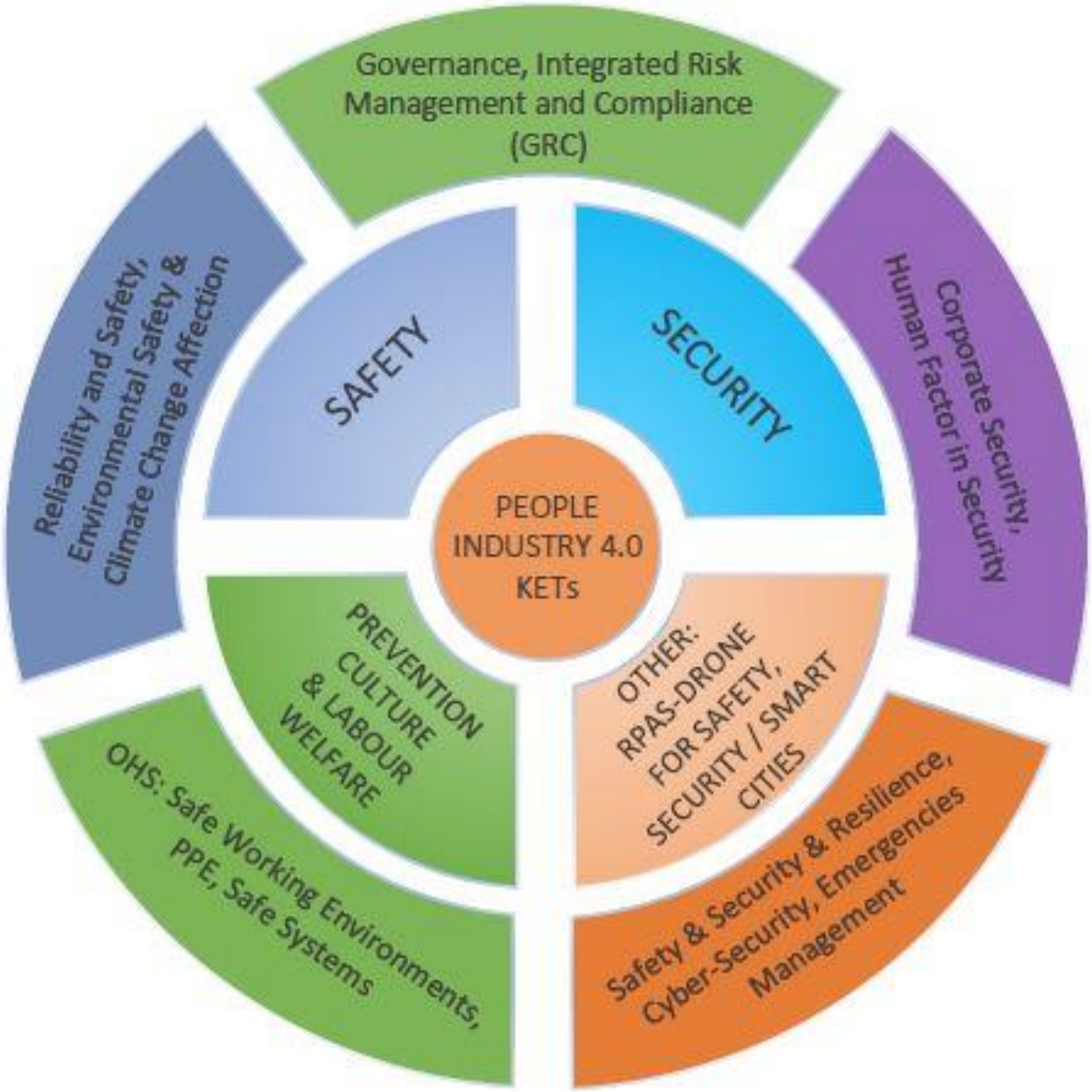
OSH: Safe working environments, PPE, safety systems,… (towards corporate wellbeing)

Security in ETPIS SafeFuture & SafeInfrastructures strategy

- **Safety and Health at work 4.0**(processes)
  - Smart Working Environments (**Worker 4.0, Wearables**…)
  - Civil Protection & Emergencies
- **Asset mangement** (ageing of infrastructures and extend life-time)
  - Sensoring, inspection technologies, structural HMS
  - New materials and smart components (cyber-physical systems…)
  - Engineering techniques, maintenance & repairment
- **Safety and reliability**:
  - Inherent safety and Risk-based design, PLM, RAMS, BIM…
  - Modelling systems, Digital tweens, DSS…
- **Protection** (critical and no-critical infrastructures)
  - Security issues
  - **CyberSecurity** (ICS, SCADA, Wearables…)
- **IT/OT & Industry 4.0** (technology evolution: challenges & threats)
- **Governance, Risk Mgt. and Resilience** :
  - **Disasters** (natural, accidents, evacuation, cascading effects on CI)
  - Dependencies between **Operators** (resilience, cascading effects)
  - **PPP on Urban Resilience (cooperation with Municipalities/Regions)**

ETPIS: updated FGs for H2020 since 2019 (PESI Secretariat)




Governance, Integrated Risk Management and Compliance (GRC)
Reliability and Safety, Environmental Safety & Climate Change Affection
SAFETY
SECURITY
Corporate Security, Human Factor in Security
PEOPLE
INDUSTRY 4.0
KETs
PREVENTION CULTURE & LABOUR WELFARE
OTHER: RPAS-DRONE FOR SAFETY, SECURITY / SMART CITIES
OHS: Safe Working Environments, PPE, Safe Systems
Safety & Security & Resilience, Cyber-Security, Emergencies Management

Security issues and CIP

Security & Resilience related to "Industrial" Critical Infrastructures

Integral Security and Resilience: the new paradigm

- World context: Security and Defence
  - New threats with new means (intelligence, cyber-arms)
- National Strategies (USA, EU) on Security and Critical Infrastructures Protection (CIP) Directives:
  - **Convergence from a National Security (& Defence) vision :**
    - Risk Analysis, physical and logical security plans
    - Military technologies (dual use) for Corporate Security
  - **CIP of "private-operated" critical or relevant Infrastructures (industrial plants / energy / oil & gas/ water/ transport inf.&networks/ telecomms…)**
    - complex industrial installations &infraestructures (more than HQ buildings and IS)
    - Cybersecurity (IS but mainly SCADA)
    - Business Continuity and Resilience
- New driver: Disaster Resilience (climate change increasing nat.disasters)
- **Smart & Secure Cities**: our Citizens and infrastructures are the new target (NY, Madrid, London, Paris & Brussels)

H-2020 – Secure Societies, next call: INFRA topics

SU-INFRA-01: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructures in Europe

- **Critical Infrastructures (for the Smart City**): Water Systems, Energy Infrastructure (power plants and distribution), Transport Infrastructure and means, Communication Infrastructure, Health Services, Financial Services

SU-INFRA-02: Security for smart and safe cities, including for public spaces

DISASTER RESILIENCE : safeguarding and securing society, including adapting to climate change (Response, Awareness/Civil protection, Communication Systems, Bio threats, CBRN cluster)

DIGITAL SECURITY:

- Cyber Security for SMEs and Individuals, Security Economics, EU and International Coordination in Cybersecurity Research and Innovation, Cyber Security Threats and Threat Actor, Privacy and Data Protection

Framework for corporate security in Spain: National Security Strategy & CIP Law

Deployment of the National CIP Law (CNPIC):

- Sectors & Critical Infrastructures :
  - Private Operators
  - Public Administrations
- Sectoral White-Books (13: 8 industry-related)
- PSO Operator Security Plan
- PPE Specific Protection Plans (individual CIs)
- Entreprise Security Organization and Plans
  - New integrated Strategy & Risk management (adaptation of Saf-Sec systems & plans)
  - Certification of Sec plans/systems (CNPIC)

+ New Law for Security Private Services (security subcontractors in Operators)

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 of industrial installations, infrastructures and networks
    - Information Security (IT-OT: Cybersecurity)
  - **GRC Strategy** & organization based on a real **SECURITY-SAFETY integration**
- New Framework (CIP Directive & National Laws, H-2020/Security):
  - **Convergence** safety- security (from different visions: industrial safety, cybersecurity and corporate security): integrated **Risk Mgt**. and **Dependencies**
  - **DRS** (Natural Disasters Resilience, including climate change) and Tech. Accidents (Civil Protection and emergencies plans): **Crisis Mgt**.
  - Critical Infraestructuras **Protection** (industry / utilities/ transport /…) towards BC
  - **Cybersecurity** (IS security, automation& control systems/SCADA)
  - **Business (essential services) Continuity and Resilience**

PESI integrated approach

Risk Management, Business Continuity and Resilience (considering Dependencies)

Risk Management and Risk concept evolution

Conventional Risk concept:

- Threat / hazard – Vulnerability – Consequences

Risk Management (ISO 31000)

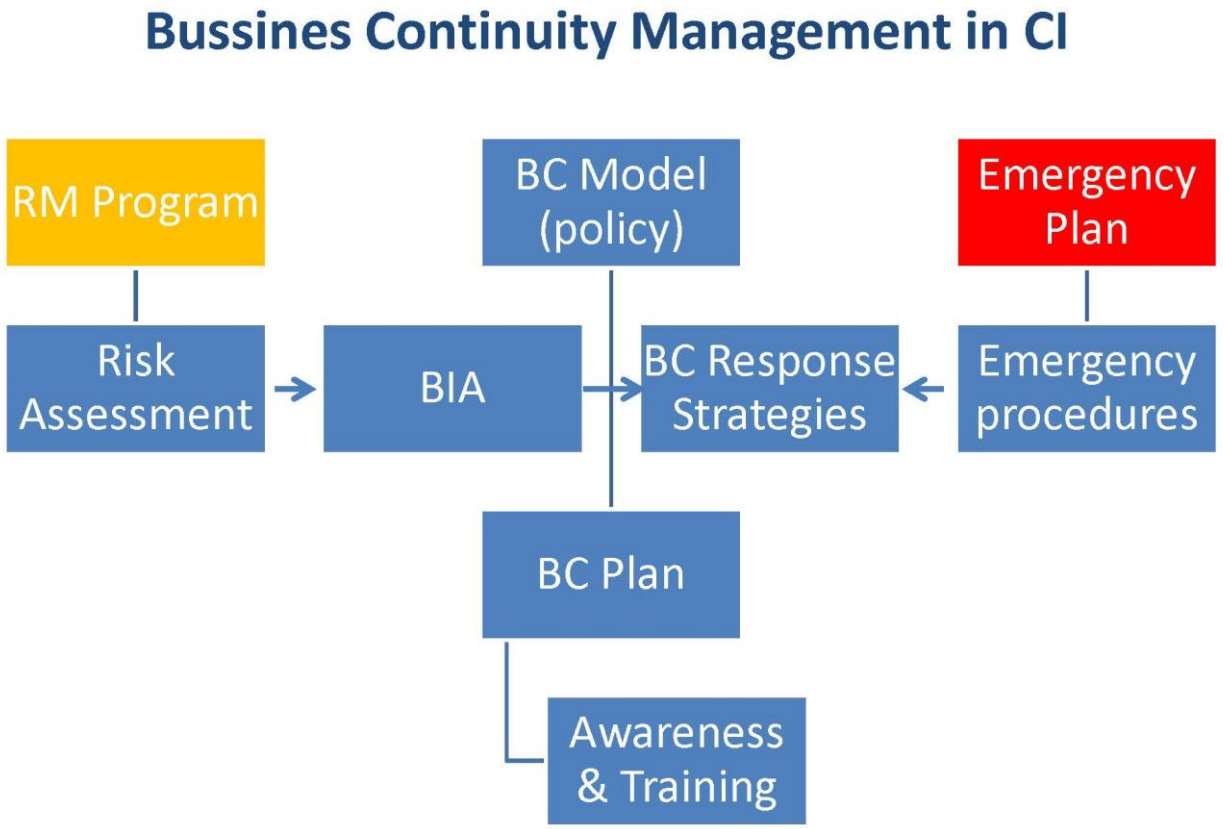
Resilience capability in an advanced Risk concept:

- Threat / hazard – Vulnerability – **Resilience** – Consequences
- Resilience: Processes/Systems/Services

Resilient People (2 layers: Individual & Teams)

PESI integrated approach for BC and Resilience in CI

Integrated Risk Management and Emergency Mgt. within an advanced Business Continuity Model



RA and BIA (Dependencies assesment)

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

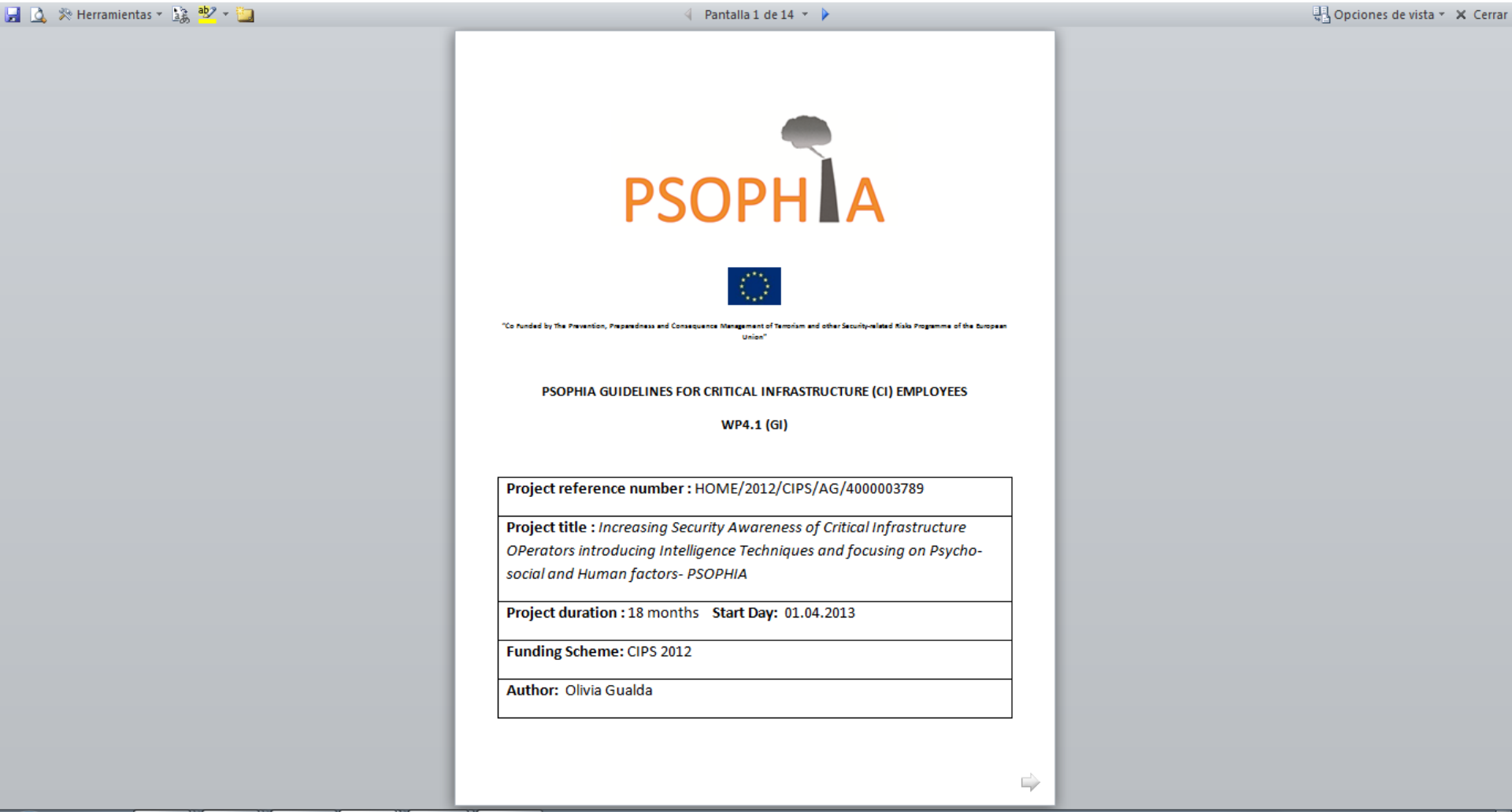
Criticity evaluation (10 categories) and Dependencies

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)																

Inter-dependencies (critical elements) with external CI

Categories	INTER-DEPENDENCIES / Critical Elements of the CI	Direct Impacts	Energy	Gas/oil	Water	Telecoms (voice, data &ISP)	Location & Environment	Transport Infrast. (road, train	Logistics (& purveyance)	Security, Civil Protection & Emergencies	Others
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)										

PESI contribution to CI Security: PSOPHIA (Personnel Security & social Engineering)



Herramientas · Pantalla 1 de 14 · Opciones de vista · Cerrar

PSOPHIA

"Co Funded by The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme of the European Union"

PSOPHIA GUIDELINES FOR CRITICAL INFRASTRUCTURE (CI) EMPLOYEES

WP4.1 (GI)

Project reference number : HOME/2012/CIPS/AG/4000003789
Project title : *Increasing Security Awareness of Critical Infrastructure OPerators introducing Intelligence Techniques and focusing on Psycho-social and Human factors- PSOPHIA*
Project duration : 18 months **Start Day:** 01.04.2013
Funding Scheme: CIPS 2012
Author: Olivia Gualda

ES 10:56 10/09/2015

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 coordinateb by Governments and Operators)
  - depedencies not based on an in-detail analysis for all active elements in the CI network/system (previous experiencies…)
  - Sec Plans and related information considered "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**: 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)

Thank you so much for your attention:

Questions or comments ?

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

PESI: technology challenges on (industrial) Security

Some priorities in R&D and innovation:

- **Convergence** model for corporate security & resilience in industrial environments and infrastructures (***Secu.Safety***)
- **Secu.Safety by design**: new methodologies and techniques
- New integrated **Risk Analysis** tools (criticity and **dependencies**)
- **Scenario simulation for integral Safety-Security,** under a multi-risk multi-factor approach: natural risks and technology/ industrial risks, for industrial zones surrounding Cities (population, civil protection and emergencies Mgt.)
- **Cyber-security (SCADA):** tools, new generation ICS, maturity models…
- **Systems Integration and Interoperability**: production systems (alarms, process control) and security (access, CCTV…): integrated **Control Centres**
- **Personnel Security** (CI Operators: privacy issues)
- **Safety Transport (hazardous materials, mass t.) & Logistics Security**: transport inf. and networks, value-chain, vehicles, interaction, routes, etc.
- **Smart grids** (electricity): standarization of Security issues
- …
- **Business Continuity and Resilience** (modelling and indicators)
- **PPP between Cities/Regions & CI Operators on Security & Resilience**

PESI - FG Security: relevant initiatives on Security

- Launching **FG-Security**:
  - Integral Security & Resilience, Cybersecurity (automation systems)
- **European R&D projects in Security Services & Resilience** (Regional/City Gov., LEAs, Security Services and Corporate Security Dept.)
  - INNOSEC, INSEC (PESI members: coordinators & partners)
  - HARMONISE …
- **INGRID Laboratories by TECNALIA**: Cybersecurity on Smart Grids (IBERDROLA and Spanish Smart-Meters & energy systems Manufacturers)
- Creation of the **CCI (Industrial Cybersecurity Center)**: Maturity model (adopted by German Cert. bodies: DEKRA, TÜV Nord…)
- **PSOPHIA Project (DGHOME): Human Factor** in Security (CI Op.)
- +20 R&D projects funded by Spanish R&D Funds
- 2015 Security Calls: Spain nº 1 in returns (grants)
- Promoting FG on Safety-Security Integration

PESI: 2016/2019 events related to Security & CIP

European Commission: "*Infoday H2020 Secure Societies: CIP*"

- PESI hosting the event (Bilbao, 8 March-2016)

CDTI-PESI: National Infoday H2020 Secure Societies (Madrid, 2016/17/18)

EC-DGs: evaluation of a ***Joint Initiative on Safety-Security integration*** *Promoters:* ETPIS, EADS, EOS, IMG-S (Brussels, 13 May 2016)

European Resilient Regions (Scotland, Lombardy-Milan, Rome, Basque C.): CIP & Resilience Network, JRC and DGHOME (Bilbao, 13-14 June 2016)

European Cong. S2R Forum: Safety & Security Research in Europe

- (Bilbao, 26-28 Oct-2016)

CRITIS-2017 (ETPIS-PESI Strategy: integrated Safety-Security-Cyber)

SMI2G (H2020 Security calls): brokerage and project proposals presentations (Brussels, February 2016/2017/2018/2019)

DG HOME CoU (Community of Users): DRS funded projects (Resilience models) (since September 2017; next March-2019)

ETPIS SafeFuture & H-2020 PPPs (related to Safety-Security integration, Resilience and CIP)

European Technology Platform on
Industrial Safety
Safety for Sustainable European Industry Growth

PLATAFORMA TECNOLÓGICA ESPAÑOLA DE SEGURIDAD INDUSTRIAL

SafeFuture

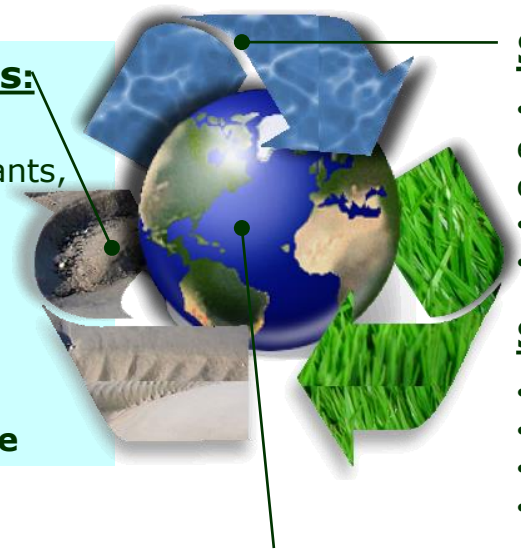
Safety as a trade-mark of the technology "made in EU"

Safe innovation for sustainable future

Way to achieving (by 2020) a new safety paradigm for European industry. Safety as a key factor for successful business and an inherent element of business performance. Industrial safety performance progressively and measurably improved in terms of reduction of reportable accidents at work, occupational diseases, environmental incidents and accident-related production losses. "Incident elimination" and "learning from failures" cultures embedded in design, maintenance, operation at all levels in enterprises. Structured self-regulated safety programs in all major industry sectors in all European countries. Measurable performance targets for accident elimination and accident free mind set workplaces as the norm in Europe.

Safe Infrastructures:

- Safe Life extension of process plants, power plants, transport & utility infra-structure networks, …
- Intensification of NatCat (NaTech)
- Design and monitoring for long term operation
- **Reliability & Resilience**



Safe Energy:

- New safety challenges in renewable energies (wind, H2, solar, bio-fuels, fuel cells, photovoltaic,…)
- Safe energy production and storage
- Smart grids

Safe Products/Production :

- Green jobs
- Value chain and interdependencies
- Nanosafety
- PPEs & Smart Working Environments

Resilience: Protection and Cyber-security

Example: Multi-Risk / Risk-Risk tradeoffs – safety for sustainable integration, interaction and risk governance:

- "Agreed Approach to Risk-Risk Tradeoff management" (the Multi-Risk initiative); difficulties in putting together different risk mitigation policies and ensuring their compatibility

Safety and Reliability: added challenges

- **Systems, Process and life-time modelling integration:**
  - SHM structural health monitoring
  - Sensoring & Inspection systems
  - Design & engineering methods (inherent safety)
  - RAMS (Reliability-Availability-Maintenance-Safety)
  - Assest /process modelling (life-time), advanced DSS
  - New issues: Security and protection
- **Information Systems (IT/OT)**
  - Software maintenance (ageing/upgrading: risky processes)
  - IT/OT evolution (IoT, Big-data, cloud comp., cyber-physical s.
  - Cyber-security (increasing threats)
- **Resiliance and Business continuity models**
  - New tools for: RM, BCM and Resilience

Instrumentation and Monitorization

- **Monitorization of processes / machines**
  - Monitorización y control de variables (sensores, instrumentación, sistemas)
  - Control remoto: sistemas y comunicaciones (GPRS, WiFi, etc.)
  - Transición desde sistemas propietarios hacia aplicaciones en tecnología Web y en la "nube"
- **New problems on Security:**
  - Sistemas embebidos (componentes)
  - Sistemas abiertos
  - Ciberseguridad