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
Indice

• **ETPIS PESI: European & Spanish Technology Platforms (2002) on integral Industrial Safety**
  – Safe & Secure Cities (under CIP: protection of Industrial & Transport Critical Infrastructures)

• **Deployment areas: Industrial Safety, OSH, Reliable Operation, Natural Disasters/Climate Change affection, Security and Cybersecurity**

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

• **Security, Resilience and Critical Infrastructures Protection (Secure Communities)**
  – Technological priorities in Industry, Networks and relevant Infrastructures
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)

Four (4) deployment areas:

• Safety (processes, installations)
• Occupational Safety & Health
• Environmental Safety (SHE) (+climate change influence on infrastructures)
• 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 Universities

4.- Other relevant institutions
- Asociación Española de Normalización (AENOR)
- Insurance, Prevention & Medical services: accidents at work, professional diseases

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 Environments, Structural Safety & ageing infrastr. –industrial plants, transport infrastructures & utility networks-, RAMS, PLM, BIM…)*
- **Human & Organizational Factors** *(safety culture, Road safety at work,…)*
- **Corporate Security** *(CIP, resilience, business continuity and industrial cybersec.)*
- **Inter-Platforms Groups: Nanosafety, Digitalization, CROBOT, RPAS/Drones**
- **IPG on Smart & Resilient City** *(Safety/Security/Cyber, Crisis Mgt., Disasters & Climate Change, Mobility, Circular Economy…)*

<table>
<thead>
<tr>
<th>HORIZON-2020</th>
<th>INDUSTRIAL LEADERSHIP</th>
<th>SOCIETAL CHALLENGES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ETPIS (PESI): New Focussed Groups</strong></td>
<td>ITC NANO BIO MAT PROD SPACE</td>
<td>HEALTH FOOD ENERGY TRANS CLIMATE SEC-SOC</td>
</tr>
<tr>
<td>SafeFuture</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>ERANET (SAFERA)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safe-Production (&amp;Safety Products)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Safe-Energy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safe-Infrastructures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety Transport (haz. goods)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security: convergence with Safety (&amp; CIP - Infrastructures Protection-)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Emergencies</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>- Cibersecurity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nanosafety &amp; Nano-toxicology (Joint ETP Group)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Environmental Safety</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Ageing at Work (Healthy &amp; Active Ageing)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Road Safety (at work)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Prevention Culture &amp; Training</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 (jointly with FG-Security; natural disasters & climate change)
  – 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 Autumn 2018): Paradigm, Tech. for Safe Mobility, ITS, Secure Transport, Hazardous goods transportation
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 infrastructures related to essential services).
SafeFuture

Safety as a trade-mark of the technology “made in EU”
Safe innovation for sustainable future

Safe Infrastructures:
• Safe Life extension of process plants, power plants, transport & utility infrastructure 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

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

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: 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 objectives 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**.
  - 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)

Decision and action

- Analysis and knowledge extraction
- Artifical Intelligence
  - Expert Systems, Soft-computing, Data-mining, Model generation
- Communication and process
- Software Architectures
  - Middleware, Databases, Cloud, Distributed Systems
- Data acquisition
- Embedded Systems
  - Sensors, Industrial electronics
  - Data acquisition protocols, Signal Processing

Behaviour modelisation (Markov nets, Altarica, etc…)

(PESI-ETPIS: H2020 Safety and Resilience, EU-OSHA Campaign (Brussels, 6 March 2019))
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 affection

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

People (safety-security culture) Industry 4.0 & Enabling Technologies

Safety-Security & Resilience Plans (business continuity, Cl 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)

(Javier Larrañeta, ETPIS Board & PESI S.G.)
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 management** (ageing infrastructures/extend lifetime, Natural disasters/CC)
  - 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, Integration (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)
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 &infrastructures (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: R&D 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

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 responsibilities 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

  – 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

Bussines Continuity Management in CI

- RM Program
- Risk Assessment
- BC Model (policy)
- BIA
- BC Response Strategies
- Emergency Plan
- Emergency procedures
- BC Plan
- Awareness & Training

(Javier Larrañeta, ETPIS Board & PESI S.G.)

PESI-ETPIS: H2020 Safety and Resilience, EU-OSHA Campaign (Brussels, 6 March 2019)
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

<table>
<thead>
<tr>
<th>Category</th>
<th>Critical Elements of the CI</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Control Rooms (Operation, Security, Integral)</td>
</tr>
<tr>
<td>II</td>
<td>Information Systems (OT/IT, ciberseg.) &amp; Communications (voice, radio, IP, ...)</td>
</tr>
<tr>
<td>III</td>
<td>Staff - Mgmt Board &amp; Crisis Committee</td>
</tr>
<tr>
<td>IV</td>
<td>- essential Teams (Op&amp;Maint, Emerg, ITC)</td>
</tr>
<tr>
<td></td>
<td>- other personnel &amp; subcontractors</td>
</tr>
<tr>
<td>V</td>
<td>Critical Processes [industrial/essential service, restricted areas... safety systems]</td>
</tr>
<tr>
<td>IV</td>
<td>Critical Process-2</td>
</tr>
<tr>
<td>IV</td>
<td>Critical Process-n</td>
</tr>
<tr>
<td>V</td>
<td>Security Equipment &amp; Systems</td>
</tr>
<tr>
<td>VI</td>
<td>Equipment &amp; appliances (essential)</td>
</tr>
<tr>
<td>VII</td>
<td>Infrastructure (buildings, installations)</td>
</tr>
<tr>
<td>VIII</td>
<td>External Services &amp; Supplies (Subcontr&amp;Providers)</td>
</tr>
<tr>
<td>IX-X</td>
<td>Others (economic, legal, Soc accept., specific)</td>
</tr>
</tbody>
</table>
# Inter-depencies (critical elements) with external CI

<table>
<thead>
<tr>
<th>Categories</th>
<th>Critical Elements of the CI</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Control Rooms (Operation, Security, Integral)</td>
</tr>
<tr>
<td>I</td>
<td>- Security Control Rooms</td>
</tr>
<tr>
<td>II</td>
<td>Information Systems (OT/IT, ciberseg.) &amp; Communications (voice, radio, IP,...)</td>
</tr>
<tr>
<td>III</td>
<td>Staff - Crisis Committee</td>
</tr>
<tr>
<td>III</td>
<td>- essential teams (Op&amp;Maint, Emerg, ITC)</td>
</tr>
<tr>
<td>III</td>
<td>- other personnel &amp; subcontractors</td>
</tr>
<tr>
<td>IV</td>
<td>Critical Processes (Industrial/essential service, restricted areas..., design, organization, tasks, safety systems)</td>
</tr>
<tr>
<td>IV</td>
<td>Critical Process - 2</td>
</tr>
<tr>
<td>IV</td>
<td>Critical Process - n</td>
</tr>
<tr>
<td>V</td>
<td>Security Equipment &amp; Systems</td>
</tr>
<tr>
<td>VI</td>
<td>Equipment &amp; appliances (essential)</td>
</tr>
<tr>
<td>VII</td>
<td>Infrastructure (buildings, installations)</td>
</tr>
<tr>
<td>VIII</td>
<td>External Services &amp; Supplies (Subcontr&amp;Providers)</td>
</tr>
<tr>
<td>IX</td>
<td>Economic &amp; Legal (Stability); Societal acceptance</td>
</tr>
<tr>
<td>X</td>
<td>Others (specific in the CI)</td>
</tr>
</tbody>
</table>
PESI contribution to CI Security: PSOPHIA
(Personnel Security & social Engineering)
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)
  – dependencies not based on an in-detail analysis for all active elements in the CI network/system (previous experiences…)
  – 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-exercises
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