Home Office

NPL National Physical Laboratory

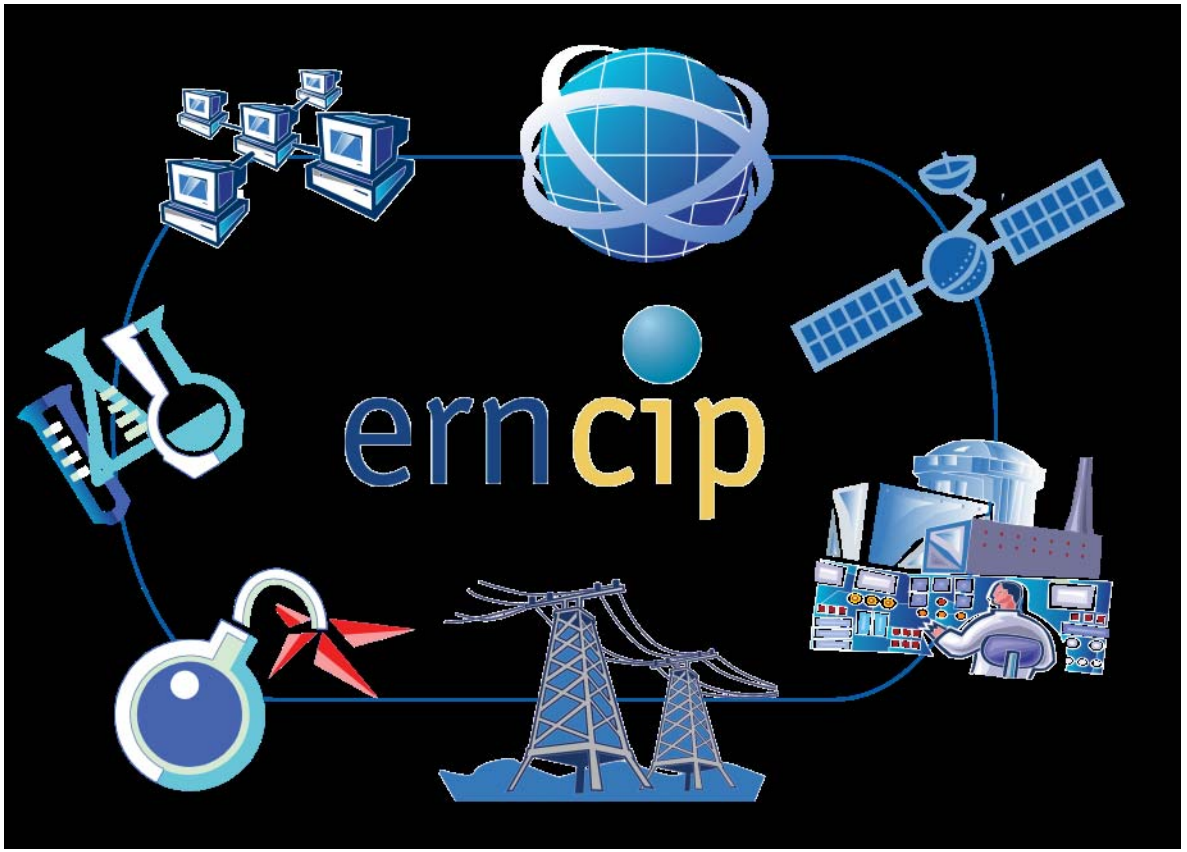
ERNCIP:

a European approach to standardisation and testing of systems for protection of critical infrastructures

Tony Mansfield (NPL) and Marek Rejman-Greene (CAST)

2 April 2014

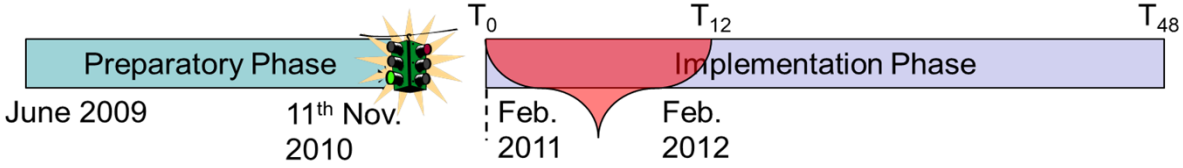
Further information



http://ipsc.jrc.ec.europa.eu/?id=688

ERNCIP – background

- European Reference Network for Critical Infrastructure Protection
- Managed by EC Joint Research Centre (JRC)
- Preparatory Phase: June 2009 – Nov 2010
- ERNCIP 4 year Implementation Feb 2011 – Jan 2015
  - Proposals in preparation for further implementation beyond 2015
  - depends on funding availability in Horizon 2020
- 9 Thematic Groups, including one on use of biometrics
- No research funding available
  - Aim is to build on activities already being undertaken by members
- Building links with NIST



Why?

- Europe has a close-meshed network of Critical Infrastructures (CIs),
  - essential for the maintenance of vital societal functions,
  - the disruption or destruction of which would have a significant impact as a result of the failure to maintain those functions
  - failure of one CI might induce risks to others and possibly failure across national borders
- CIs are exposed to multiple threats having many facets
  - Cybercrime, terrorism, natural disasters
- Increased vulnerability of Critical Infrastructures to unintended technological failure – can they be made more resilient?

- … more

Why?

- Europe has a close-meshed network of Critical Infrastructures (CIs),
  - essential for the maintenance of vital societal functions,
  - the disruption or destruction of which would have a significant impact as a result of the failure to maintain those functions
  - failure of one CI might induce risks to others and possibly failure across national borders
- CIs are exposed to multiple threats having many facets
  - Cybercrime, terrorism, natural disasters
- Increased vulnerability of Critical Infrastructures to unintended technological failure – can they be made more resilient?
- Traditional security solutions
  - national markets: standardised products
  - International markets: highly specific solutions
- But lack of EU wide conformity assessment
  - for security-related equipment and systems, services and applications
  - seen as a barrier to development, hinders market acceptance of products

ERNCIP mission

To foster the emergence of innovative, **qualified**, efficient and competitive **security solutions**, through the networking of European **experimental capabilities**

… specifics in next slide

ERNCIP mission

To foster the emergence of innovative, **qualified**, efficient and competitive **security solutions**, through the networking of European **experimental capabilities**

Qualified – access to certified & accredited facilities and related expertise

Security solutions – such as laboratory availability, certifications, labelling, best practices, relative dissemination, testing practices, etc

Experimental capabilities – complete and exhaustive suite of experimental facilities, methods and knowledge to suit the needs of ERNCIP stakeholders

to increase availability & networking of EU experimental facilities & laboratories

- ERNCIP aims to provide a framework within which
  - experimental facilities and laboratories share knowledge & expertise to
    - identify security products & solutions
    - harmonise test protocols and measurements
    - explore the possibility of EU-wide certification
    - make recommendations for research and investment
- Delivery mechanisms
  - Inventory of test laboratories offering specific capabilities
    - database managed by EU's Joint Research Centre at Ispra, Italy
  - 9 Thematic Groups, one of which is Applied Biometrics for CIP

Thematic Groups

- Aviation Security Detection Equipment
- Explosives Detection Equipment (non-Aviation)
- Industry Control Systems (ICS) and Smart grids
- Structural Resistance against Seismic Risks
- Resistance of structures against Explosion effects
- Chemical & Biological Risks in the Water Sector
- Video Analytics and Surveillance
- **Applied Biometrics for CI Protection**
- Nuclear and radiological threats to critical infrastructure

Membership of biometrics TG

- ~ 20 members
- 8 countries & representation from European Commission
- 7 active participants in ISO standards committees

- Critical Infrastructure Protection authorities
- technology suppliers
- integrator
- SME
- test houses
- universities and research institutions

Opportunities for testing biometric systems

Common Test Protocols:

- Recommend common test methodologies and protocols for testing
- Develop new test methodologies & harmonise existing ones
- Promote standardisation of test methods via CEN, CENELEC etc
- Investigate the possibility of drafting EU-wide recommendations for products/ solutions that may improve the protection/resilience of critical infrastructure or mitigate the risk

Certification

- Investigate possibility & conditions of promoting a common certification or labelling procedure
- Recommend an EU-wide evaluation / certification / labelling procedure
- Recommend an EU-wide qualification scheme for labs that wish to evaluate such products / solutions

Range of potential applications Biometrics in critical infrastructures

- physical access control
- logical access control
- ‘on the spot’ verification of identity
- Automated Border Control gates/systems
- verification against biometric identity documents
- surveillance
- vetting – criminal record check
- audit of key/critical actions in operation of facilities
- confirmation of specialised training and qualifications
- ensure integrity of critical components in CI networks/facilities
  - documentation, biometric feature and digital signature

Biometric TG Activities

1. work on raising awareness, promotion of appropriate use of biometrics in CIs, and elicitation of priorities
   - guide to use of biometrics
   - assessment of priorities amongst CI operators
2. standardisation, evaluation, testing and certification of selected applications to meet the requirements of operators of CIs
   - Standards profiles for Automated Border Control systems ('e-gates') – *European Commission mandate M/487*
   - Access control (access to specific rooms inside buildings)
   - Biometric recognition of individuals from CCTV
   - Logical access control and mobile identity checks

Thank you for your attention

Questions?

Tony.Mansfield @ npl.co.uk

Marek.Rejman-Greene @ homeoffice.gsi.gov.uk

NPL National Physical Laboratory

Home Office

Centre for Applied Science and Technology