

Press Release

5th February 2010

Risk Governance Framework required to manage threats to critical energy infrastructure

The security and economy of the European Union, and the well-being of its citizens, depends on shared critical infrastructure measures, according to a report published by AEA for the European Commission (Directorate-General Justice Freedom and Security). The report urges European organizations running critical infrastructure to implement a new Risk Governance Framework which applies common standards across Europe.

AEA's Jonathan Perks, principal author of the report, said:

"The interconnected world we live in today is increasingly reliant on ICT to support our Critical Infrastructure. Common European standards are essential to avert disaster and guarantee economic and social stability."

"The domino effect of the recent banking crisis highlighted the need for reassurance to national and regional government organizations. Groups operating and regulating key national and regional infrastructures must have adequate risk governance frameworks in place, not only to protect their own business continuity but also the wider communities."

Within the EU energy supply system, transfers of energy are largely conducted through shared infrastructures. They are increasingly interconnected, complex and reliant on ICT systems for control and instrumentation of the networks as well as business management. Furthermore, as the use of ICT in both operational and business systems grows such as smart metering for electricity distribution, there is a tendency to become more reliant on common systems and commercial off-the-shelf IT technologies.

Failure of a Critical Energy Infrastructure in one country can lead to significant disruption of supplies in one or more Member States and also cascade not only into the energy sector but through into other critical sectors. In 2006, for example, 15 million households across Europe as well as the German railway system were affected by a fault in Germany which cascaded along the network, bringing widespread disruption and infrastructure risk.

The study has investigated the vulnerability of critical energy infrastructures dependent on ICT systems for ensuring the security oil, gas and electricity. According to the report, due to the lack of storage and real time control required, the failure of electrical supply systems will have the most

rapid and wide-ranging impact. Without electricity, all forms of transport are quickly affected as control systems (traffic lights, rail signals) and communications systems cease to operate. Water and sewage systems stop when pumps and controls are not operating and financial systems cease to function without modern communications equipment.

A common European approach is required where infrastructure in one Member State could cause significant impacts in other Member States. In this case private or national decision processes may not have adequate information or motivation to undertake investments which are more justifiable from a wider perspective.

The study, carried out by AEA in partnership with Risk Solutions, ESR Technology and Dialogik, for the European Commission, proposes a new Risk Governance Framework so that key stakeholders responsible for managing the European energy supply systems can identify, communicate and manage risks which could result from the failure of ICT systems and which may have significant impact on European energy supplies in several Member States.

- Ends -

The report, Study on Risk Governance of European Critical Infrastructures in the ICT and Energy Sector can be found on

http://ec.europa.eu/energy/infrastructure/studies/doc/2009_10_risk_governance_report.pdf

Notes to Editors:

For more information contact:

Michael Evans/Rowan Baker

Madano Partnership

020 7593 4000

www.madano.com

Jo Wheeler

AEA PR Manager –

0870 190 2799

jo.wheeler@aeat.co.uk

About AEA

AEA is a leading energy and climate change consultancy. We work with the UK Government, the EU and major private sector organisations around the world to address the challenges of climate change, energy management, sustainability, air and water quality, resource efficiency and transport. Our multi-disciplinary team of over 1,000 technical and scientific consultants, project management experts, information technology professionals, and legal and regulatory specialists enable us to deliver fully integrated solutions for our customers. We prepare the National Atmospheric Emissions Inventory and

the Greenhouse Gas Inventory for the UK Government (web-enabled at www.naei.org.uk). We were also cited by the United Nations for our contribution to the Nobel Peace Prize awarded to Al Gore and the Intergovernmental Panel on Climate Change. For more information please visit www.aeat.co.uk

About Risk Solutions

Risk Solutions origins stem from developing and applying state of the art risk management methods in the nuclear energy and chemical process industries. Risks Solutions is a team of strategic thinkers, with a strong analytical grounding across several business sectors, including rail and road transport, central government, and energy, with proven project management capabilities, working closely with both clients and key project stakeholders. They provide controls assurance and risk management consultancy services to a wide range of clients.

About DIALOGIK

DIALOGIK brings special competence and experience into the proposed project with regard to the conceptual-analytical design of risk governance issues for security issues. DIALOGIK has acted as the coordinator of the PrecauPri-project which developed a policy framework for precautionary and participatory risk regulation in Europe (which was tested using new organic chemicals as a case study) and as coordinator of that subproject of the Safe Foods project which was entrusted with the investigation of institutional challenges and solutions to the implementation of a food safety governance system which is more inclusive and integrative in these terms: by building on both natural scientific expertise and social scientific expertise as well as systematic and experiential knowledge, and by involving the four major actors in risk decision making, i.e. political, business, scientific and civil society players, in the process of framing the problem, generating options, evaluating options, and coming to a joint conclusion.

About ESR Technology

ESR Technology (ESRT) was formerly the Engineering, Safety and Risk business of AEA Technology. ESRT incorporates all the expertise, staff and facilities from that business and thus brings a heritage of more than 40 years experience of the application of engineering excellence to demanding projects. ESRT continues to specialise in the provision of independent technical expertise, products and services to help their Customers: Ensure Asset Integrity, Improve Machine Reliability, Manage Safety & Risk, and Transfer Best Practice. ESRT's highly skilled, world-class consultancy teams have in-depth experience of working with Customers across many sectors, including: Oil & Gas; Rail; Utilities; Aviation; Space and Defence

Background on European Programme for Critical Infrastructure Protection (EPCIP)

On 17-18 June 2004, the European Council asked the Commission to prepare an overall strategy to enhance the protection of critical infrastructures¹. In response, the Commission transmitted on 22 October 2004 a Communication entitled "Critical Infrastructure Protection in the Fight against Terrorism"² putting forward suggestions to enhance European prevention, preparedness and response to terrorist attacks involving critical infrastructures (CI).

The Commission's intention to propose a European Programme for Critical Infrastructure Protection (EPCIP) and a Critical Infrastructure Warning Information Network (CIWIN) was accepted by the 16-17 December 2004 European Council³ in the Council conclusions on prevention, preparedness and response to terrorist attacks⁴ and in the Solidarity Programme⁵, both adopted by the Council on 2 December 2004.

Throughout 2005, intensive work was done on the elaboration of EPCIP. Two European seminars on critical infrastructure protection and a number of informal meetings were held bringing together experts from all EU Member States. This work culminated in the adoption by the Commission on 17 November 2005 of the Green Paper on a European Programme for Critical Infrastructure Protection (COM (2005) 576 final).

The Green Paper exercise was followed by a detailed impact assessment and the adoption on the 12 th of December 2006 of a policy package on EPCIP composed of a communication and a Directive. The communication deals with general policy in connection with EPCIP (CIWIN, work-streams to develop EPCIP, sectoral interdependencies, annual work planning and the residual work on National Critical Infrastructure) whereas the Directive focuses on the designation of critical infrastructure of a European dimension (European Critical Infrastructure or "ECI").

More information at http://ec.europa.eu/justice_home/funding/2004_2007/epcip/funding_epcip_en.htm