



7.Çerçeve Programı Bilgi ve İletişim Teknolojileri ve Güvenlik Alanı Ortak 1. Çağrı Konuları

Activity/ Area	Topics called	Funding Schemes
<i>ICT THEME</i>		
<i>Pervasive and Trusted Network and Service Infrastructures / Critical Infrastructure Protection</i>	ICT-SEC-2007.1.7: Technology building blocks for creating, monitoring and managing secure, resilient and always available information infrastructures that link critical infrastructures	<i>Collaborative project and Coordination and support action</i>

Activity/ Area	Topics called	Funding Schemes
<i>SECURITY THEME</i>		
<i>Security systems integration, inter-connectivity and interoperability</i>	Topic ICT-SEC-2007-1.0-01 Risk assessment and contingency planning for interconnected transport or energy networks	<i>Collaborative project and Coordination and support action</i>
	Topic ICT-SEC-2007-1.0-02 Modelling and simulation for training	<i>Collaborative project</i>
	Topic ICT-SEC-2007-1.0-03 Optimised situational awareness through intelligent surveillance of interconnected transport or energy infrastructures	
	Topic ICT-SEC-2007-1.0-04 ICT support for first responders in crises occurring in critical infrastructures	

Objective ICT-SEC-2007.1.7: Critical Infrastructure Protection

(Joint Call between ICT and Security Themes FP7-ICT-SEC-2007-1)

The interoperability and interconnectivity of supply systems is one of the cornerstones of the functioning of our societies. The vulnerabilities in the intercommunication of systems, equipment, services and processes and their resilience against malicious attacks of terrorism and (organised) crime are elementary to the security of the citizens. The objective of the joint call is to make key infrastructures of modern life, such as energy production sites and transmission systems, storage and distribution, information and communication networks, sensitive manufacturing plants, banking and finance, healthcare, or transportation systems more secure and dependable. The aim is to protect such critical infrastructures that can be damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, mismanagements, accidents, computer hacking, criminal activity and malicious behaviour and to safeguard them against incidents, malfunctions and failures.



7.Çerçeve Programı Bilgi ve İletişim Teknolojileri ve Güvenlik Alanı Ortak 1. Çağrı Konuları

The joint call is structured around two specific foci.

1. Focus of the ICT Theme

The first focus is called for by the *ICT* theme and is addressing technology building blocks for creating, monitoring and managing secure, resilient and always available information infrastructures that link critical infrastructures so that they survive malicious attacks or accidental failures, guarantee integrity of data and continuous provision of responsive and trustworthy services, and support dynamically varying trust requirements. This includes:

- a) Understanding and managing the interactions and complexity of interdependent critical infrastructures; mastering their vulnerabilities; preventing against cascading effects; providing recovery and continuity in critical scenarios (including research towards designing and building self-adapted and self-healing complex systems); security and dependability metrics and assurance methods for quantifying infrastructure interdependencies.
- b) Designing and developing secure and resilient networked and distributed information and process control systems; systemic risk analysis and security configuration and management of critical information infrastructures and dynamic assurance frameworks for interconnecting them with critical infrastructures; availability of security forensics.
- c) Developing longer term visions and research roadmaps; metrics and benchmarks for comparative evaluation in support of certification and standardisation; international cooperation and co-ordination with developed countries; coordination with related national or regional programmes or initiatives.

Funding schemes: a) and b): CP (STREP only); c) CSA

2. Focus of the Security Theme

The second focus is called for by the Security theme¹³ and is addressing technology building blocks for creating, monitoring and managing secure, resilient and always available transport and energy infrastructures that survive malicious attacks or accidental failures and guaranteeing continuous provision of services. The following topics are called:

Topic ICT-SEC-2007-1.0-01: Risk assessment and contingency planning for interconnected transport or energy networks

Technical content / scope: The task is to develop integrated frameworks and agreed, common methodologies for (a) global analyses and assessment of risks, failures and vulnerabilities of transport or energy infrastructures, and (b) management and contingency planning based on the compilation and analyses of emergency plans, to ensure interoperability between interconnected and interdependent heterogeneous transport or energy infrastructures.



7.Çerçeve Programı Bilgi ve İletişim Teknolojileri ve Güvenlik Alanı Ortak 1. Çağrı Konuları

Funding scheme(s): Collaborative project and Coordination and support action (aiming at supporting research activities).

Topic ICT-SEC-2007-1.0-02: Modelling and simulation for training

Technical content / scope: Security crises concerning cross-border interconnected European transport or energy infrastructures can lead to effects with high impacts of disruption. The task consists of modelling & simulation including scenario building for handling security incidents to support the training of crisis managers.

Funding scheme(s): Collaborative project.

Topic ICT-SEC-2007-1.0-03: Optimised situational awareness through intelligent surveillance of interconnected transport or energy infrastructures

Technical content / scope: The task consists of developing tools that integrate smart surveillance information from interconnected and heterogeneous transport or energy infrastructures in order to build up high-level situation awareness. The objective is to enable optimized decision-making required for cross-border interoperable crisis management to ensure secure, resilient and always available transport or energy infrastructures.

Funding scheme(s): Collaborative project.

Topic ICT-SEC-2007-1.0-04: ICT support for first responders in crises occurring in critical infrastructures

Technical content / scope: The task consists of developing novel technologies for personal digital support systems as part of an integral, secure emergency management system to support first responders in crises occurring in various types of critical infrastructures under all circumstances. The action has to build upon ongoing research on emergency management, secure wireless communication, first responder technologies, etc. See as well topic SEC-2007-

4.3.03 Personal equipment with a view to compatibility and complementarity¹⁶.

Funding scheme(s): Collaborative project.

Expected impact:

- Significant improvement in the security, performance, dependability and resilience of complex and interdependent critical infrastructures while considering as well organisational dynamics, human factors, societal issues and related legal aspects.
- Reinforce European industry's potential to create important market opportunities and establish leadership.



7.Çerçeve Programı Bilgi ve İletişim Teknolojileri ve Güvenlik Alanı Ortak 1. Çağrı Konuları

- Contribution to establishing, strengthening and preserving trust in the use of technologies for the protection of critical infrastructures. This includes creating sufficient awareness and understanding of all relevant issues for the take-up of their outcome (e.g. regarding potential classification requirements, international co-operation needs, communication and implementation strategies etc.), in order to ensure acceptance of such technologies by relevant stakeholders.

- More effective protection through enhanced co-operation, coordination and focus across Europe, and contribution to the development and promotion of metrics, standards, evaluation and certification methods and best practice in security of critical infrastructures. Indicative budget distribution

40 M€: 20 M€ for specific focus 1 provided by the ICT theme and 20 M€ for specific focus 2 provided by the Security theme.

- A minimum of 90% of the call budget is foreseen to be allocated to collaborative projects of a typical size in the range of 2-5 M€ (total cost) and a duration of 2-4 years.

- Up to 10 % of the call budget is foreseen to be allocated to coordination and support actions (CSAs) of an average size of 0.5 M€.

- Out of the Security theme's budget, an indicative 1 M€ is available for international cooperation.