**Partner Search Form**

### 1. Project Proposal Information

<table>
<thead>
<tr>
<th><strong>Project Proposal Title</strong></th>
<th>Self-Informed Perimeter Protection Dual System for Counter Terrorism</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Project Proposal Acronym</strong></td>
<td>S.I.-Dual-Sy.</td>
</tr>
<tr>
<td><strong>Call Identifier</strong></td>
<td>CIP-01-2016-2017</td>
</tr>
<tr>
<td><strong>Topic(s)</strong></td>
<td>Critical Structures; Counter-terrorism; physics and cyber protection; automatic sistema</td>
</tr>
<tr>
<td><strong>Funding Scheme</strong></td>
<td>IA - Innovation</td>
</tr>
<tr>
<td><strong>Keywords</strong></td>
<td>Counter-terrorism electronic systems; automated systems; cyber network protection; underwater acoustic; mag systems and sensors; data merge, storage, interpretation, representation.</td>
</tr>
</tbody>
</table>

### Abstract (Max. 2000 words)

The S.I.-Dual-Sy. Project
Self-Informed Perimeter Protection Dual System for Counter Terrorism

**An answer to the call:**

**Innovative Technical Features**

Self-informed protocol of environmental mag measure (metrology of singularity), increasing of the confidence of the counter-terrorism detection measure (from 15-30% to > 97%), capacity of detection in critical infrastructures proximity, very high noise areas and high traffic flow areas (uw and land environment), first application (counter-terrorism) on civil environment, passive protection of large areas without interference with human activities

**Rationale**

- Introduction
Today’s political scenario raises urgent issues about citizen security in terms of counter-terrorism, involving Western countries in general and EU in particular. When focusing on the specific needs for critical infrastructure protection, the S.I.-Dual-Sy. Project addresses issues related to transportation security and the freedom of movement for the citizens (especially ports), as well as energy production assets such as electric power plants.
- State of the art
The S.I.-Dual-Sy. proposal stems from consolidated previous results in the area of Defense projects. These activities lead to a novel integrated system, with land-maritime applications, for the high-accuracy detection of intruders in the presence of high noise, both acoustic and electro-magnetic (EM). The project combines specialized methods for physical structure protection with innovative tools and methods for the protection of the cyber dimension. From a physical viewpoint, the approach has proved most effective in several domains, namely, marine port/harbor environments, land-based scenarios such as extra-urban or high-traffic urban sites, and high EM noise such as power plants. The S.I.-Dual-Sy. design, test and validation phases rely on: new-generation UW/land magnetic sensors (most of which have been suitably developed), a novel defense-derived system with self-informed capability of magnetic intrusion detection, which has been successfully tested in divers detection applications and preliminary applied to land-based scenarios, as well. See for reference the EU project HaPS granted by European Defence Agency (R.SWE Navy, ITA Navy, R.Norwegian Navy, German Navy) and the C.A.In.M.N and La.Ma.-1.0 projects, funded by the Italian Ministry of Defence.

A basic service of the cyber component of the integrated system is to ensure the protection of communications between sensors and the various system elements; conventional tools are used for that purpose. For the specific cyber protection of ports and land sites, however, a novelty point of the project consists in the support to proactive intelligence, for the early detection of (asymmetric) threats by continuous, active monitoring of the cyber space. This is done by means of specialized tools that have already been developed and tested, and are currently being used for prevention and event monitoring by Law Enforcement Agencies.

- Short description of the S.I.-Dual-Sy. project

**Physical security component**
The project covers the design, manufacturing and validation of an automated monitoring system for counterterrorism, relying on a self-informed magnetic measurement strategy (Fig.1), which integrates with acoustic sensors.

The self-informed magnetic measurement (also denoted as singularity measurement) is a method for the detection of variations in the magnetic field first developed for military applications. The project represents the first deployment of the integrated technologies in non-military domains, and refers to a scenario of asymmetric threats; it operates in both underwater (UW) and land environments. In the UW version, it combines a magnetic-based and an acoustic-based subsystems, whereas the land version only includes the magnetic component. The magnetic approach greatly increases the confidence (accuracy) in intrusion detection and enhances operational impact in high-noise areas, such as ports and perimeter access sites (Faggioni et
A key tool consists in handy electronic device (\(\geq 10x5x2\) [cm]) providing access code for identifying, authenticating and authorizing armed security operators.

The S.I.-Dual-Sy supports automated monitoring and reporting of the attempt of unauthorized access, and can manage possible reaction countermeasures, at increasing levels of impact: a plain alarm level, a non-lethal reaction level with indirect means (including intrusion spot lighting, acoustic/optical/gas interference, up to military deployment against the intruder.

**Cyber security component**

The integrated system develops a network for the distributed security monitoring in a spectrum of critical infrastructures, and propagates operational information at three timing levels: First Order level, local Security Authorities that are responsible for the threatened site; Second Order, National-level Security Agencies; Finally, European-level coordination Institutions. Thus intrusion timing and site information can be readily made available to all interested parties in a secure and timely manner (Fig. 2). The cyber component adopts state-of-art cryptographic algorithms and protocols to ensure the protection of data, information, and their related transmission to all active parties, from sensors all the way to centralized EU organisms. This schema includes the set-up of authorization strategies, layered access control, and secure logging. In addition, novel and dedicated technologies are deployed for the active exploration of the cyber space, in order to support proactive intelligence and provide early detection of incoming threats. This is accomplished by using advanced methods for semantic information processing and monitoring of social networks/deep web, which have already been successfully tested and deployed, and will be further improved for the specific application scenario at hand.

**Advantages and results**

The project enforces security for the automated control of transit by armed/unarmed personnel in remote or near areas. This applies to both high-noise maritime/land sites and high-density traffic access. The approach allows a theoretically unbounded operational range and a resulting containment or mitigation of the asymmetric assault risk. In particular, at the external interface border of the critical structure being protected, the S.I.-Dual-Sy. supports automated and remote control of hostile/friendly traffic, so that human supervisors are timely alerted about risks before reaching physical proximity with the threat.

**Key concepts**

- High-confidence detection of armed hostile intrusions to traffic-intensive areas, and/or in the presence of high noise, related to critical infrastructures (ports, power plants, urban sites);
- Remote control (protection of security operators)
- Automated reaction upon alerts (assisted by operator governance of
modular reaction)
- integrated multi-layer flow of information and knowledge (from peripheral monitors to EU-centralized institutions)
- Cyber protection of data, information, and communications
- Proactive intelligence for cyberspace monitoring and early detection of threats
- Authentication and monitoring of operators at access points

Source projects
Ha.P.S.
Harbor- Base Protection System, EDA European Defence Agency (SWE, ITA. GER, NOR), Brusselles, 2010-13
C.A.I.Ma.N.
La.Ma.-1.0
Land/Marine Magnetometric Detector for Selfinformed Networks, MINDIFE Italian Ministry of Defence, Roma, 2014

A short bibliography


### Partner Search Form

| Current Consortium (Partners, Organisation Types) | (Preliminary)  
WP1 – Project scientific governance and administration; WP2 – Mag subsystem and sensors; WP3 – Acou subsystem and sensors; WP4 – S.I.-Dual-Sy. Mag-Acou integration; WP5 – S.I.-Dual-Sy. Networks integration; WP6 – cyberg information flux protection, system cyber attack protection.  
(At 19.03.16)  
ITA (Institutional and Industrial Partners; Partnership closed)  
SPA (Institutional; Partnership open) |
| Deadline for Responses | 30.4.2016 |

### 2. Profile of the Partners Sought

| Organisation Type | Institutional (Scientific, Military and Civil Security Organizations, Civil Administrations, ……); Critical Structures Management Authorities (Harbor, Power Plants, Structures for the transport and storage of hydrocarbons, ……..), Industrial (competence see “keywords” and “abstract”) |
| Required Skills and Expertise | Acoustic, Electronics, TLC, cybernetic, data acquisition – merge – representation, critical strcture management |
| Role in the project | Partners |
| Other Requirements | Expertise in management and governance of harbors and power plants will be the owners and system operators (end user) |

### 3. Project Proposer Information

| Name of the Organisation | SkyTech S.r.l. via delle Pianazze, 74 - 19136 La Spezia (SP) - Italy |
| Organisation Type | Industrial company |
| Country | ITA |
| Fields of Activity | Electronics; remote controls and observations (space, land and uw) |
## Partner Search Form

<table>
<thead>
<tr>
<th>Contact Person</th>
<th>Alessandro Carbone / Maurizio Forcieri (Proposal Manager)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second contact person (institutional): Osvaldo Faggioni, Project Scientist in Charge, Università di Genova – DITEN SEALab, <a href="mailto:osvaldo.faggioni@unige.it">osvaldo.faggioni@unige.it</a></td>
<td></td>
</tr>
<tr>
<td><strong>Position in the Organisation</strong></td>
<td>CEO / President</td>
</tr>
<tr>
<td><strong>Tel</strong></td>
<td>+39.0187.984100; fax.: +39.0187.943528</td>
</tr>
<tr>
<td><strong>Email</strong></td>
<td><a href="mailto:carbone.a@skytechnologies.it">carbone.a@skytechnologies.it</a> / <a href="mailto:forcieri.m@skytechnologies.it">forcieri.m@skytechnologies.it</a></td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="http://www.skytechnologies.it">www.skytechnologies.it</a></td>
</tr>
<tr>
<td><strong>Previous Projects Participated</strong></td>
<td>(in security theme)</td>
</tr>
<tr>
<td>La.Ma.-1.0 (Land-Marine Magnetometric Detector for Selfinformed Networks)</td>
<td></td>
</tr>
</tbody>
</table>