|  |  |
| --- | --- |
| **Titlu proiect (Română)** | **Securitatea cibernetică și reziliența infrastructurilor critice** |
| **Titlu proiect (Engleză)** | **Cyber security and resilience of networked critical infrastructures** |
| **Acronim** | **SERENITI** |
| **Nr. contract** | **PCIG14-GA-2013-631128** |
| **Finanțator** | **Seventh Framework Programme of the European Union** |
| **Program** | **Marie Curie Career Integration Grant (CIG)** |
| **Director proiect** | **Conf. dr.ing. GENGE Béla** |
| **Data începere** | **01 Martie 2014** |
| **Data terminare** | **29 Februarie 2018** |
| **Pagina Web** | [**http://upm.ro/sereniti/**](http://upm.ro/sereniti/) |

**Scurt rezumat**

Conform directivei 114 din 2008 a Comisiei Europene, sistemele de energie (gaze naturale, electricitate, petrol) sunt considerate ca fiind infrastructuri critice. Aceste infrastructuri asigură funcționarea normală a societății noastre și în consecință, protejarea lor în fața atacurilor cibernetice tot mai frecvente reprezintă o problemă de securitate atât Europeană cât și națională. Proiectul intitulat Cyber Security and Resilience of Networked Critical Infrastructures (SERENITI) își propune să elaboreze soluții inovative pentru proiectarea infrastructurilor critice (IC) cu cerințe de securitate și reziliență. Noutatea proiectului constă în îmbinarea dimensiunii fizice a IC cu dimensiunea cibernetică, un aspect ce lipsește cu precădere din metodele existente. Proiectul va duce la dezvoltarea unor metode avansate de protejare a IC, la dezvoltarea sistemelor noi de detectare a anomaliilor și intrușilor. Proiectul se încadrează în contextul descris de politicile Europene “European Programme for Critical Infrastructure Protection” (EPCIP), planul de acțiune “Critical Information Infrastructure Protection” (CIIP) și “Digital Agenda for Europe” (DAE).

Proiectul adresează o serie de goluri din literatura de specialitate incluzând:

* Metode inovative pentru proiectarea IC cu cerințe de securitate și reziliență.
* Un sistem distribuit pentru detectarea intrușilor care fuzionează dimensiunea cibernetică de dimensiunea fizică a acestor infrastructuri.
* O nouă metodă de proiectare a rețelelor de detectare a intrușilor pentru IC.

Desfășurarea proiectului este structurată pe două faze:

Faza 1: Martie 2014 – Februarie 2016: elaborarea de metode pentru proiectarea rețelelor de comunicație a IC cu cerințe de securitate și reziliență. În această fază au fost dezvoltate metode matematice pentru proiectarea optimală a rețelelor IC incluzând cerințe specifice de securitate și reziliență conform standardelor industriale IEC/IEEE. Metodele au fost publicate într-o serie de publicații științifice de specialitate (conferințe și reviste), precum și softuri accesibile de pe pagina Web a proiectului.

Faza 2: Martie 2016 – Februarie 2018: elaborarea de metode pentru detecția intrușilor și pentru proiectarea rețelelor de comunicație a sistemelor de acest tip. În această fază s-au elaborat metodele matematice (clustering, fuzionare a datelor) pentru detectarea anomaliilor în sistemele de comunicație ale IC, precum și metode de optimizare matematică pentru poziționarea optimală a acestor detectoare. Rezultatele au fost publicate într-o serie de conferințe și reviste de specialitate.

**Indicatori realizați până în Octombrie 2016:**

1. Publicații în Reviste ISI cu Factor de Impact:

4 publicații în reviste ISI (<http://upm.ro/sereniti/publications.html>) cu factor de impact (1 revistă **ISI Roșu** FI = 2.114, 3 reviste **ISI Galben**, FI = 1.351).

1. Publicații (principale) în cadrul unor conferințe internaționale:

Peste 10 articole publicate în conferințe de specialitate (<http://upm.ro/sereniti/publications.html>):

* CRITIS 2016: Paris, Franța.
* SmartGift 2016: Liverpool, Marea Britanie.
* IEEE/IFIP Networking 2016: Viena, Austria.
* ISDFS 2014, ISDFS 2016: Houston, Texas, SUA.
* INDIN 2015: Cambridge, Marea Britanie.
* ICCIP 2015, 2016: Washington DC, SUA.
* ADHOC-NOW, 2015: Athena, Grecia.
* EuroSec, 2014: Amsterdam, Olanda.

1. Premii:

**Best Paper Award**: IEEE International Conference on Industrial Informatics, 22-24 July 2015, Cambridge, UK, 2015 (lucrarea: *A Clustering-based Approach to Detect Cyber Attacks in Process Control Systems*).

**IEEE Industrial Electronics Society (IES) 2015 Best Paper Award:** Lucrarea *“A Clustering-based Approach to Detect Cyber Attacks in Process Control Systems”* a primit premiul pentru cea mai reprezentativă lucrare pe anul 2015 pentru toate conferințele organizate de IES în 2015.

**Premiul I la Positive Hack Days (PHDays):** Kiss István (membru al proiectului) a obținut premiul I la Positive Hack Days, Moscova (Mai 26-27, 2015) pentru prezentarea unui nou tip de atac.

**Premii UEFISCDI:** două lucrări premiate de UEFISCDI (premierea articolelor).

1. Dezvoltarea de instrumente software:

**Cyber-security-aware network design tool-suite for Networked Critical Infrastructures**. Disponibil on-line: <http://upm.ro/sereniti/netdesign.html>

**OptimalFlow: A Hierarchical Control Plane for Software-Defined Networks-based Industrial Control Systems.** Disponibil on-line: <http://upm.ro/sereniti/optimalflow.html>