

A research engineer fellow position is available in the ISID (Ingénierie des Systèmes d'Information et de décision) group of the CEDRIC Laboratory (<https://cedric.cnam.fr/>).

The successful applicant will join the european project SAFECARE.

The position is for 18 months. It is available immediately and will remain open until filled.

Interested applicants should contact me at [ilham.lammari@lecnam.net](mailto:ilham.lammari@lecnam.net) , and in any case before February 29.

The description of the required profil is given bellow

-----  
Context:

This research engineer position takes place within the EU H2020 SAFECARE project (SAFEguard of Critical heAlth infrastructure). The aim of this project is to provide solutions that will improve both physical and cyber security in a cost-effective way. Also, it will promote new technologies and novel approaches to enhance threat prevention, threat detection, incident response and mitigation of impacts.

Nowadays, the lines between physical and cyber worlds are increasingly blurred. Almost all equipment is connected to the Internet, and physical intrusion might affect cyber security. Threats cannot be analyzed separately as physical or cyber, and therefore it is critical to develop an integrated approach in order to fight against such a combination of threats.

One of the main objectives of SAFECARE is to propose a model that formalizes the cascading effect of an incident in the context of e-health. Based on this model, it will be possible to anticipate the potential impacts of cyber and physical incidents, not only on building infrastructures (power supply, air cooling, etc.), but also on IT systems and medical devices. The model will be based on an ontology that describes the domain knowledge.

The recruited person will be in charge of developing an innovative ontology-based threat propagation module for e-health. He or she will participate in the project monitoring and meetings with partners.

The position tasks include:

- Ontological modeling of the SAFECARE core ontology: this task defines a conceptual model and core ontology for capturing essentially static knowledge. The conceptual model and core ontology will be refined in each of the main project phases.
- Ontological modeling of the impact management: this task extends the core ontology mentioned above with the definition of concepts that are essential to impact propagation computation. It also provides indicators to help deciding about the suitable countermeasures to face attacks consequences.
- Definition and implementation of IPM rules: this task defines and creates the IPM (impact propagation module) rules used to automatically infer the impact propagation.
- Continuous integration of results: this task consists of the continuous integration of the developed components into the global cyber-physical security solutions.
- Test and demonstration: this task tests the developed prototype on a test platform in order to validate that it is operational and tests its interconnections with other solutions before

implementation in real operational environments.

- Dissemination and communication: this task disseminates and exploits the project results throughout the health-user and scientific community.

Requirements:

Candidates will hold a Master degree or a PhD degree in Computer science or a related field and is able to combine theoretical and practical aspects in his/her work. Fluent English communication, ability to work in an international network of collaborators, and software technology skills are fundamental requirements. The candidate should have a background in at least one of the following fields:

- Semantic web technologies
- Knowledge representation
- Logic, AI, automated reasoning, or related subfields

It would be a plus if the candidate has a background in cyber security field.

Full stack developing skills are required.

Duration:

18 months, starting as soon as possible.

Location:

Conservatoire National des Arts et Métiers, CEDRIC Laboratory, 2 rue Conté 75003, Paris, France

Contacts:

Faten Atigui: [faten.atigui@lecnam.net](mailto:faten.atigui@lecnam.net)

Nadira Lammari: [ilham.lammari@lecnam.net](mailto:ilham.lammari@lecnam.net)