Managing Cyber-physical Incidents Propagation in Health Services

Faten Atigui, Fayçal Hamdi, Fatma-Zohra Hannou, Nadira Lammari, Nada Mimouni, Samira Si-Said

Managing Cyber-physical Incidents Propagation in Health Services

Faten Atigui✉, Fayçal Hamdi✉, Fatma-Zohra Hannou ✉, Nadira Lammari ✉, Nada Mimouni✉, and Samira Si-said Cherfi✉

CEDRIC, Conservatoire National des Arts et Métiers (CNAM), Paris, France
{faten.atigui, faycal.hamdi, fatma-zohra.hannou, nadira.lammari, nada.mimouni, samira.cherfi}@lecnam.net

- **Full name:** Integrated cyber-physical security of health services
- **Acronym:** SAFECARE[1]
- **Duration:** from 09-01-2018 to 08-31-2021
- **URL:** https://www.safecare-project.eu/

1 Summary of the project

Health services are among the most critical and vulnerable cyber-physical infrastructures. The SAFECARE H2020 project aims to provide solutions that improve physical and cyber security in a seamless and cost-effective way.

1.1 Objectives

The goal of the project is to provide an integrated solution for the management of combined cyber and physical threats and incidents, their interconnections and potential cascading effects. The main objectives are:

- Risk assessment of physical and cyber threats, with respect to current EU regulatory bodies' requirements, and cost efficiency of proposed solutions.
- Improve risk prevention capacities: analysis of vulnerabilities, risk assessment and recommendations on operational active systems.
- Improve threat detection capacities: data fusion, cascading effects models
- Improve impact mitigation: manage hospital availability, inform the population, increase user awareness about incidents impacts on critical assets.
- Provide impact propagation and decision support model that describes cyber and physical assets, their vulnerabilities, incidents, and their impacts.

1.2 Expected Tangible Outputs

The SAFECARE project will produce the following main key results:

- A cyber threat detection system and a physical threat detection system
- A threat response system and a threat mitigation system
- A modular and scalable solution with standard communication protocols
- Dissemination throughout health-user community and scientific community
- Demonstration in three European hospitals

[1] This project has received funding from the European Union's H2020 research and innovation programme under grant agreement no. 787002

2 Current Results: Impact Propagation Module

We present in this section the current work on the core module of the SAFECARE project that is the impact propagation and decision support model (IPM). This module relies on: (i) structural information about cyber and physical assets, their intrinsic properties and theirs structural relationships, and (ii) on knowledge about the occurred incidents and how to infer and propagate impacts. This second knowledge evolves continuously and is more dynamic than the structural knowledge. To cope with the static and dynamic knowledge and to confer more stability to the IPM module, we propose a modular ontology, called Safecare-Onto. At a high level of abstraction, the whole picture is depicted in Figure 1.

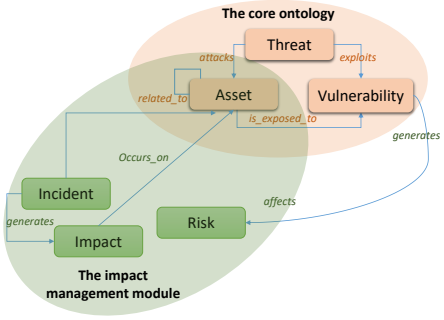

Fig. 1. The modular structure of SafecareOnto

The core ontology captures essentially the static knowledge about critical assets. It is centered on three main concepts: *Asset*, *Vulnerability*, and *Threat*.

These concepts are further refined and characterised, and their formalisation can easily be extended. Other modules could incrementally be defined upon the core ontology. The impact management module is one of the possible extensions. It defines the concepts that are essential to the computation of impact propagation and provides indicators for assessing the severity of incidents and the likelihood of impacts. It relies on concepts such as *Incident*, *Risk* and *Impact*. Other modules could also be added as a countermeasures module.

The propagation management relies on axioms and rules that are further used to infer the impact of incidents. These rules result from several threat scenarios defined with the help of cyber and physical security experts and the collaboration of actors from European hospitals partners. A first version of a prototype that we implemented simulates impacts propagation on a near-real scenario. A reasoner is used to infer impacts propagation on assets. In this prototype, the IPM rules were expressed in terms of OWL concepts (classes, properties, individuals) using the JENA rule engine.