# Semantic Systems Modeling and Monitoring for Real Time Decision Making: Results and Next Steps within the Greek Cyber Security Center of Excellence.

D. Kostopoulos, V. Tsoulkas, G. Leventakis, P. Drogkaris and V. Politopoulou

Center for Security Studies (KEMEA), Ministry of Public Order and Citizen Protection,
P. Kanellopoulou 4, Athens, GR-10177, Greece
{tsoulkas.kemea, dimkostopoulos, george.leventakis,
prokopis.drogkaris, v.politopoulou}@gmail.com

**Keywords**: Critical Infrastructures, semantic modeling, Semantic reasoning and risk analysis, core system ontologies, stream reasoning and event processing, DST user interfaces.

Our presentation is comprised of two interconnected sections: Firstly we will present results recently delivered and approved by the European Commission regarding the EC FP-7 project SERSCIS (Semantically Enhanced Resilient and Secure Critical Infrastructure Services). http://www.serscis.eu. These focus on the following issues:

- The SERSCIS Proof of Concept Architecture with the associated technical limitations during the initial implementation phase. In the sequel the concept and advantages of introducing in a later realization stage modern stream reasoning techniques and in particular the data processing steps in a stream reasoner for real time threat classification and estimation.

- The Semantic monitoring architecture with an emphasis on the Semantic Monitoring and Reasoning Components as well as the so called "Behavioral Analyser" capable of mapping the streaming monitoring data into semantic assertions about the presence or absence of a threat against a Critical Infrastructure.

- The Semantic Reasoning Process in combination with its sequential reasoning computational steps.

Moreover and in conjunction with the A-CDM approach (Airport – Collaborative Decision Making) which is the European Initiative for optimizing European Air Traffic Management across European airports, validation results will be provided. In this direction some asset threat cases will be analyzed for the SERSCIS Proof of Concept comprised of: Attacks - Induced behaviors – Controls. Semantic modeling issues will be presented in conjunction with the final prototypical Decision Support Tool Interfaces.

In the second part the recently launched ***G**reek **C**yber **S**ecurity **C**enter of **E**xcellence* will be introduced including: Its national and European dimension, it's educational and awareness role to societal needs concerning cyber-crime as well as planned research activities and efforts related to Fast Intrusion Detection algorithms and the use of Semantics dynamic modeling approaches towards state of the art cyber – security tools.

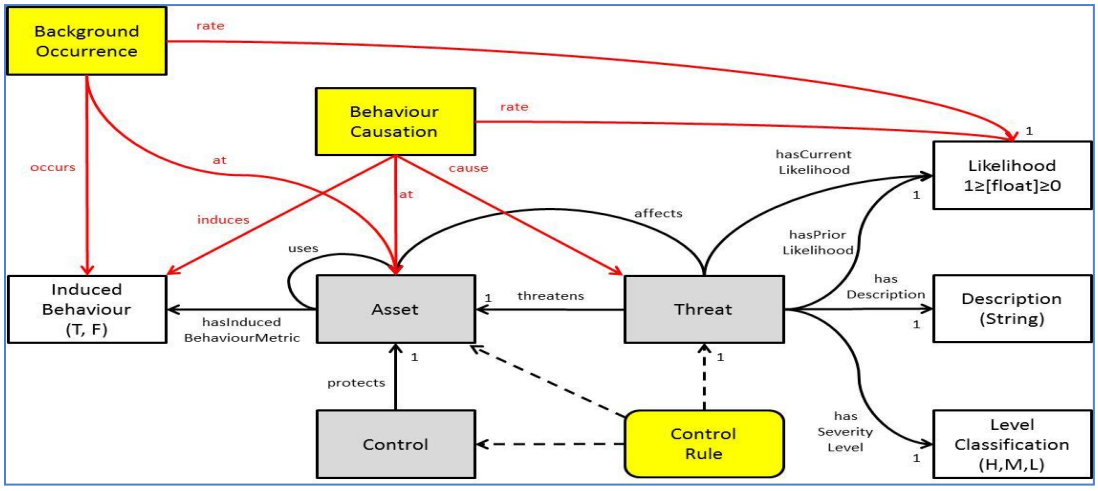


**Figure 1. Proof of concept: Complete Core Ontology**

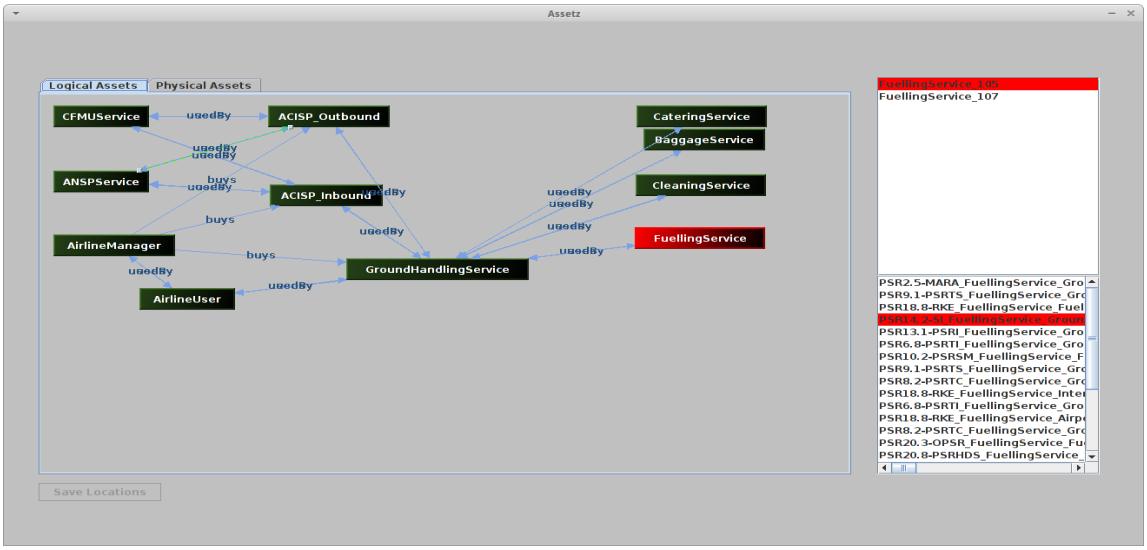


**Figure 2. Decision Support Tool Screenshot of Logical Assets with Threat Alarm.**

## References


[1] M. Surridge, A. Chakravarthy, M. Hall-May, R. Nossal: "SERSCIS: Semantic Modelling of Dynamic, Multi-Stakeholder Systems," Second SESAR Innovation Days, 27th-29th November 2012.

[2] Semantically Enhanced Resilient and Secure Critical Infrastructure Services, EC FP7 Project 225336, 2008 – 2012. (http://www.serscis.eu)

[3] Deliverable D5.2: Decision Support Tools: Full Prototype Implementation, 22/01/2013. Lead Author: Vasilis Tsoulkas. Contributors: D. Kostopoulos, N. Nikitakos, M. Surridge, W. Chen, T. Leonard, M. Hall-May. Internal Reviewer: M. Surridge

[4] D.F. Barbieri, D. Braga, S. Ceri, E.D. Valle and M. Grossniklaus, "Incremental Reasoning on Streams and Rich Background Knowledge," in ESWC, Heraklion, Greece, 2010.

[5] Kostopoulos, D., Leventakis, G. Tsoulkas, V., and Nikitakos, N., "An Intelligent Fault Monitoring and Risk Management Tool for Complex Critical Infrastructures: The SERSCIS Approach in Air-traffic Surface Control, In: *14th International Conference on Computer Modelling and Simulation (UKSim)*, March 2012, Cambridge, UK (IEEE Computer Society).