

Vladimír Soběslav

University of Hradec Králové,
Czech Republic



TITLE

Cybersecurity in Smart Cities: Integrating Process and Ontological Modeling, Security Baselines, and Experimental Validation

ABSTRACT

This lecture presents research and applied activities aimed at strengthening cybersecurity in Smart City environments through the integration of security-oriented process modeling, ontological knowledge representation, security baselines, and experimental validation of selected concepts. Process modeling enables formalized descriptions of cyber-incident handling procedures, service interdependencies, and coordinated response workflows across interconnected urban domains. Ontology-based representations further capture semantic relationships among assets, threats, security controls, and organizational contexts, thereby supporting interoperability, reasoning, and informed governance-level decision-making. The contribution further defines and evaluates security baselines that establish consistent minimum protection requirements for urban digital infrastructures. Selected methodological components are experimentally assessed in representative Smart City scenarios to examine their practical applicability and relevance for operational resilience. Together, these results improve situational awareness, support coordinated incident response, and strengthen the long-term cyber resilience of Smart City ecosystems.

CV

Vladimír Soběslav is an associate professor and researcher in computer science at the Faculty of Informatics and Management, University of Hradec Kralove, Czech Republic. His research focuses on cybersecurity, computer networks, virtualization, cloud computing, and the protection of critical information infrastructures, with particular emphasis on Smart City and energy-sector environments. He is actively involved in national and international research and innovation projects addressing cyber resilience, security architectures, ontology-driven security management, and AI-assisted threat detection. His work includes collaboration with academic institutions, public organizations, and industrial partners in the energy and cybersecurity domains. He contributes to the design of experimental cybersecurity infrastructures, knowledge-based security Systems, and methodologies for risk assessment.

