SPRING**SIM'20**

2020 Spring Simulation Conference

AIMS AND SCOPE

Real-world applications have been always the driving force for the development of Modeling and Simulation (M&S) theories. For over 50 years, the **Annual Simulation Symposium (ANSS) Track** has been a forum to exchange ideas, results, and methods related to real-world theories and applications of M&S for Simulationists in industry, government, and academia. The purpose of this track is to highlight and advance rigorous experimental, computational practices of M&S devoted to the study of real-world problems. Research on all topics concerning the practice of M&S theories are welcome. Authors are invited to present research of all kinds, including case studies and applications. Recommended topics in the track include, but are not limited to, the following with application to real-world problems:

- Advances in the field of M&S for implementation purposes
- Application of modeling formalisms into real-world applications
- Rigorous comparisons across M&S techniques
- New applications of M&S
- Novel uses of M&S in real world applications
- Application of M&S to co-design, hardware-in-the-loop, co-simulation
- M&S tools: performance analysis, scalability

SUB-TRACKS

Humans, Societies and Artificial Agents (HSAA)

Artificial societies have typically relied on agent-based models, Geographical Information Systems (GIS), or cellular automata to capture the decision-making processes of individuals in relation to places and/or social interactions. This has supported a wide range of applications (e.g., in archaeology, economics, geography, psychology, political science, or health) and research tasks (e.g., what-if scenarios or predictive models, models to guide data collection). Several opportunities have recently emerged that augment the capacity of artificial societies at capturing complex human and social behavior. Mixed-methods and hybrid approaches now enable the use of 'big data', for instance by combining machine learning with artificial societies to explore the model's output (i.e., artificial societies as input to machine learning), define the model structure (i.e. machine learning as a preliminary to designing artificial societies), or run a model efficiently (i.e. machine learning as a proxy or surrogate to artificial societies). Datasets are also broader in type since artificial societies can now be built from text, or generate textual as well as visual outputs to better engage end-users. Authors are encouraged to submit papers in the following areas:

- Applications of artificial societies (e.g., modeling group decisions and collective behaviors, emergence of social structures and norms, dynamics of social networks)
- Data collection for artificial societies (e.g., using simulations to identify data gaps, population simulations with multiple data sources, use of the Internet-of-Things)
- Design and implementation of artificial agents and societies (e.g., case studies, analyses of moral and ethical considerations)
- Participatory modeling and simulation
- Policy development and evaluation through simulations
- Predictive models of social behavior
- Simulations of societies as public educational tools
- Mixed-methods (e.g., analyzing or generating text data with artificial societies, combining machine learning and artificial societies)

- Models of individual decision-making, mobility patterns, or socio-environmental interactions
- Testbeds and environments to facilitate artificial society development
- Tools and methods (e.g., agent-based models, case-based modeling, soft systems)

Complex, Intelligent, Adaptive and Autonomous Systems (CIAAS)

Heterogeneous systems are the norm today. A system deployed in a net centric environment eventually becomes a part of a system of systems (SoS). This SoS also incorporates adaptive and autonomous elements (such as systems that have different levels of autonomy and situated behavior). This makes design, analysis and testing for the system-at-hand a complex endeavor. Testing in isolation is not the same as a real-system operation, since the system's behavior is also determined by the input, which evolves from the environment. This exact factor is difficult to predict, due to an ever-increasing level of autonomy. Advanced Modeling and Simulation (M&S) frameworks are required to facilitate SoS design, development, testing, and integration. In more particular, these frameworks must provide methods to deal with intelligent, emergent, and adaptive behavior as well as autonomy. The subject of emergent behavior and M&S of emergent behaviors takes the center stage in such systems as it is unknown how a system responds in the face of emergent behavior arising out of interactions with other complex systems. Intelligent behavior is also defined as an emergent property in some complex systems. Consequently, systems that respond and adapt to such behaviors may be called intelligent systems as well. Topics of interest include, but are not limited to:

- Methodologies, tools, and architectures for adaptive control systems
- Knowledge engineering, generation and management in CIAAS
- Weak and Strong emergent behavior, Emergent Engineering
- Complex adaptive systems engineering
- Self-* (organization, explanation, configuration) capability and collaborative behavior in CIAAS
- Live, Virtual and Constructive (LVC) environments
- Modeling, engineering, testing and verification of complex behavior
- Complexity in model engineering of complex SoS
- Metrics for Complexity design and evaluation
- Verification, validation and accreditation of Complexity in SoS

Cybersecurity Engineering (CSE)

Modeling and Simulation has the ability to improve our understanding and gain better insights into the exploitability and impact of threat landscape in cyber systems underpinning several critical infrastructures. The emergence of Internet of Everything has resulted in the growth in interactions between humans, physical and cyber systems and there is a increased need to understand how these interactions could be exploited by adversaries. Modeling and simulation provide a cost-effective means to support research, development, refinement, deployment, and evaluation of the next generation of security solutions for preventing, detecting, and recovering from cyber-attacks and failures. The goal of this track is to provide a forum to present and discuss advancements in research, tools, techniques, solutions, best practices, and heuristics related to the modeling and simulation of cybersecurity. The symposium will address all aspects of modeling, analyzing, design, simulation, implementation, deployment and management of security algorithms, protocols, architectures and systems. We encourage submissions related to all aspects of cybersecurity in a modeling and simulation context in a broad spectrum of application areas. Topics of interest include, but are not limited to:

- Formal models for cybersecurity simulation

- Cybersecurity evaluation and assessment approaches
- Testbeds and experimental infrastructure for cybersecurity simulation
- Simulation platforms for cybersecurity assessment
- Hybrid simulations for cyber physical system security
- Modeling and Analysis of Networked security systems
- Modeling security and privacy in mobile and cellular networks
- Modeling security for future Internet architectures
- Risk assessment and management
- Systems engineering for security

Cyber-Physical Systems (CPS)

Cyber Physical Systems (CPS) are complex engineered systems whose operations are controlled, coordinated, monitored, and integrated by computer-based algorithms. Examples of CPS include smart grids, autonomous automotive and avionics systems, medical monitoring and control, process control systems, robotic systems, and automatic pilot avionics. This computing power is embedded in the physical environment of a wide variety of objects and structures, and is interconnected using networks. Such tightly coupled computations and communication capabilities allow CPS to augment with physical processes with new capabilities. With the advent of low-cost programmable internet-ready hardware, CPS are rapidly becoming internet-connected. Such an Internet of Things (IoT) opens new possibilities for collecting, managing and processing large data sets to manage and control such systems at different temporal, physical, and geographical scales. Advances in the CPS and IoT domains are having great economic, social and technical impacts. Therefore, there is an emerging consensus that new methodologies and tools are needed for developing such systems. Topics of interest include, but are not limited to:

- Modeling and simulation of CPS
- Application of multi-domain and multi-formalism modeling and analysis to CPS
- Distributed and cloud computing based-implementations of complex CPS
- Design automation tools and tool chains for model-based design of CPS
- Design of networking systems for CPS
- Control of (networked) CPS
- Simulation-guided formal verification of safety-critical CPS
- Resilient and robust system design of CPS and IoT
- Ubiquitous and pervasive computing for enhanced user interactions with CPS and IoT
- Novel applications of CPS