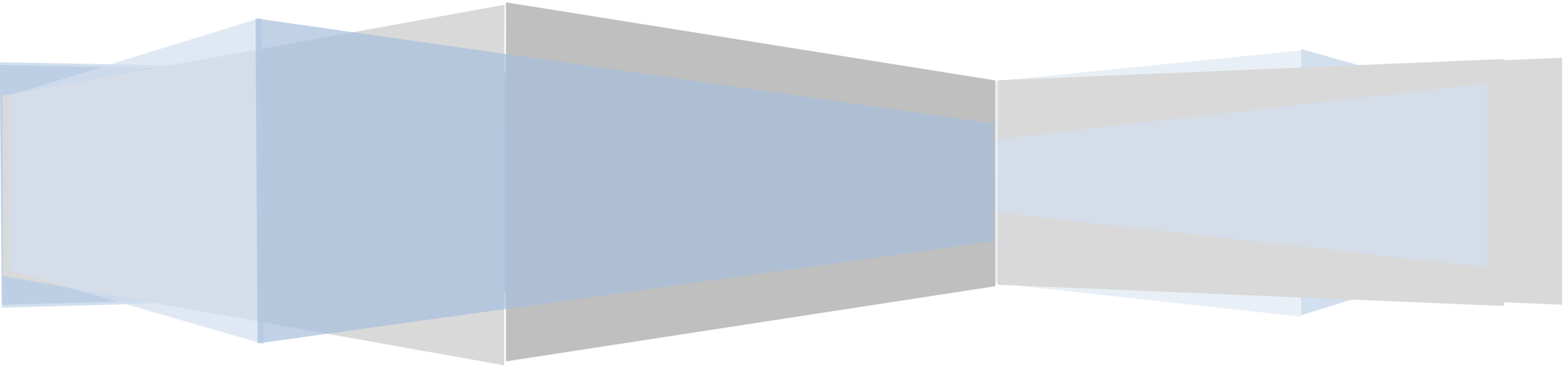
华东师范大学软件工程学院
教育部可信软件国际合作联合实验室
国家可信软件国际联合研究中心
国家软件人才国际培训基地（上海）

Trustworthy Artificial Intelligence

可信人工智能



“Trustworthy Artificial Intelligence”
SEI-Summer School 2020

		Monday	Tuesday	Wednesday	Thursday	Friday
		13, July	14, July	15, July	16, July	17, July
Morning	8:30-10:10	Shaoying Liu	Shaoying Liu	Zhiming Liu	Zhiming Liu	Sheffield Lab
		(Hiroshima University)	(Hiroshima University)	(Southwest University)	(Southwest University)	(Huawei)
	10:10-10:30	Break	Break	Break	Break	Break
	10:30-12:00	Shaoying Liu	Shaoying Liu	Zhiming Liu	Zhiming Liu	Sheffield Lab
Noon	12:00-14:00	Lunch	Lunch	Lunch	Lunch	
Afternoon	14:00-15:30	Xiaowei Huang	Xiaowei Huang	Guy Katz	Guy Katz	
		(Liverpool University)	(Liverpool University)	(The Hebrew University of Jerusalem)	(The Hebrew University of Jerusalem)	
	15:30-15:50	Break	Break	Break	Break	
	15:50-17:20	Xiaowei Huang	Xiaowei Huang	Guy Katz	Guy Katz	

Course Introduction

Software Abstractions and Human-Cyber-Physical Systems Architecture Modelling （Prof. Zhiming LIU）

Human-Cyber-Physical Systems (HCPS) is a combination of Cyber-Physical Systems (CPS) with ubiquitous computing (also known as intelligent environment) and social systems, including social computing. In HCPS, humans as individuals or unorganized and organized crowds deeply involved in interactions with physical and cyber systems, and operation and control of physical processes and hardware dynamically shift between humans and machines. The theory and methods of HCPS is still in its infancy, and research is needed to establish its scientific foundation so as to make advances in its engineering methods.

In this short course, we reflect the development of software engineering through software abstractions and show that these abstractions are integral in the notion of software system architectures. We discuss that it is important to engineer systems using formal methods in relation to the definition and management of development processes, and argue how a model of the software architecture, with rich semantics and refinement relations, plays an important role in this process. We recall the traditional separation of processes for domain modelling and software requirements modelling in model-driven software development. We then propose to combine these modelling approaches and this naturally leads to a unified process for HCPS architecture modelling, design, and evolution. Based on the unified processes, we outline a framework in engineering formal methods for HCPS modelling, with the discussion about significant challenges including integration, composition, collaboration, verification of HCPS with multi-dimensional heterogeneity. Human components, as well as all kinds of artificial intelligent systems, are particularly major courses of the heterogeneity.

Prof. Zhiming LIU (Southwest University)

Zhiming LIU has been working in the area of software theory and methods. He is known for his work on Transformational Approach to Fault-Tolerant and Real-Time Systems, Probabilistic Duration Calculus for System Dependability Analysis, and rCOS Method for Object-Oriented and Component-Based Software. Zhiming Liu studied mathematics in university. He holds a MSc in Computing Science from Software Institute of CAS (1988) and a PhD in Computer Science from University of Warwick (1991). Zhiming Liu joined Southwest University in Chongqing as a full-time professor of computer science in 2016. He is leading the development of the University Centre for Research and Innovation in Software Engineering (RISE). Before Southwest University, he worked in three universities in the UK (1988-2005 and 2013-2015) and the United Nations University – International Institute for Software Technology (Macau, 2002-2013).

Formal Verification of Deep Neural Networks (Prof. Guy Katz)

Deep neural networks have emerged as a widely used and effective means for tackling complex, real-world problems. However, a major obstacle in incorporating them as controllers in safety-critical systems is the great difficulty in providing formal guarantees about their behavior. In recent years, attempts have been made to address this obstacle by formally verifying neural networks. However, neural network verification is a computationally difficult task, and traditional verification techniques have often had only limited success - leading to the development of novel techniques. In this series of talks we will survey the state of the art in neural network verification, focusing on Satisfiability Modulo Theories (SMT) based approaches and on abstraction/refinement based methods. Additionally, we will survey recent advances in the verification of recurrent neural networks. Finally, we will discuss the applicability of neural network verification, going over examples that include airborne collision avoidance, neural network simplification, and the verification of rate control algorithms.

Prof. Guy Katz (Hebrew University of Jerusalem)

Guy Katz is an assistant professor at the Hebrew University of Jerusalem, Israel. He received his Ph.D. at the Weizmann Institute of Science in 2015. His research interests lie at the intersection between Formal Methods and Software Engineering, and in particular in the application of formal methods to software systems with components generated via machine learning.

TBD

========== THE END==========