



NATIONAL PH.D. PROGRAM IN AUTONOMOUS SYSTEMS

Fault Diagnosis and Security in Smart Cities

Ph.D. candidate

Yike Li

Cycle

XXXVIII

Tutors

Prof. Alessandro Giua

1. Description of the research program

A **smart city** is constituted by various smart systems. The risk of suffering from malicious attacks and the emphasis on security and privacy are much higher than in traditional systems. This research programs aims to investigate privacy and security problems emerging in smart cities. For sake of generality, we use formalisms like the cyber-physical system and develop methods for **fault diagnosis** and **attack prevention**. The applicability of obtained methods will be discussed on a real platform.

This program has three main purposes as below:

- Define a unified theoretical framework for smart cities

Considering the multidimensional nature of infrastructures in smart cities, we plan to propose a unified formalization that is adaptable to various systems, which is applied for further analysis.

- Propose efficient methods of fault diagnosis and privacy analysis for smart cities

To analyze the risks that may be encountered in smart cities, we use tools in system control theory to develop new methods to detect and prevent failures and attacks.

- Apply and test the developed approaches in a real application in smart cities

Select a specific infrastructure or service in smart cities, utilizing sets of modeling and analysis approaches developed by us. Further, the validation and performance of our approaches will be examined through practical application on the platform.

Based on the efforts that the system control community has made to the CPS privacy and security, our study inherits their formalization and makes innovations on it as below:

- Investigate smart cities with a unified formal perspective, which is macroscopic and adaptable for diverse multifaceted systems.
- Analyze vulnerabilities and threats more comprehensively, with respect to the heterogenous components in smart cities.
- Take human activities into account when designing the plant (as a component that constitutes the system) and analyze the unsafe factors (like mishandling).

Modeling and analysis methods are ultimately applied for the whole process of research on a real system, to ensure the research has practicability.

2. Schedule of the research activities

First academic year (planned)

	Description	Period	Activity abroad
Investigation on structure & properties of smart city	Investigate the latest technologies in smart cities, analyze the potential safety and privacy problems.	11/2022 – 02/2023	NO
Investigation on automatic control theory	Investigate the recent approaches developed by control system community.	03/2023 – 11/2023	NO

Second academic year (planned)

	Description	Period	Activity abroad
Research on novel attacks in smart cities	In the frame of smart cities, investigate the diagnosability and controllability of given system against novel attacks.	12/2023 – 02/2024	NO
Research on privacy of data in smart cities	Consider a specific data processing process like collecting, transmitting, and storage, etc, design the methods to protect the privacy.	03/2024 – 05/2024	NO

Research on systemic fault diagnosis for smart cities	Investigate the detection and prevention of systemic faults like unplanned downtime in large-scale infrastructures.	06/2024 – 08/2024	NO
Research on efficiency and economy of control approaches	Design defense strategies within limited or less expansion of the number of monitor or actuator agents.	09/2024 – 11/2024	NO

Third academic year (planned)

	Description	Period	Activity abroad
Research cooperating with BU	Collaborate with Prof. Christos Cassandras, focus the problems forwarded by him related to smart cities.	12/2024 – 05/2025	YES (Boston University, US)
Research cooperating with ARST	Collaborate with ARST, to solve the practical problems in smart city application scenarios like light metro dispatching.	06/2025 – 11/2025	NO

3. Training and research activities plan

First academic year (planned)

	Description	Period	Final Exam	ECTS
A. Ph.D. courses	Linear Algebra for Control Applications (L. Schenato)	(to be decided)	Yes	2
	Fault detection techniques in Condition Monitoring: Model-Based and Data-Driven Methods (S. Simani)	(to be decided)	Yes	1
	SIDRA PhD School	(to be decided)	Yes	4
B. Master's degree courses	Analysis and Control of Cyber Physical System (A. Giua) (with final exam)	(to be decided)	Yes	6
C. Soft skill courses	/	/	/	0
D. Participation to seminars	10 hours seminars	(to be decided)		3
E. Participation to international congresses or workshops	3 days conferences	(to be decided)		3
F. Presentation of research products at international congresses or workshops	1 presentation	(to be decided)		2
	TOTAL OF ECTS FOR TRAINING ACTIVITIES			21
G. Individual research activity	700 hours individual research activity	(to be decided)		28
H. Supervision of students	75 hours support for Master's thesis	(to be decided)		3
I. Integrative teaching activities	/	/		0
J. Preparation of manuscripts for	200 hours preparation of manuscripts for conferences or journals	(to be decided)		8

conferences or journals				
	TOTAL OF ECTS FOR RESEARCH ACTIVITIES			39
	TOTAL OF ECTS			60

Second academic year (planned)

	Description	Period	Final Exam	ECTS
A. Ph.D. courses	SIDRA PhD School	(to be decided)	Yes	4
B. Master's degree courses	Supervisory Control and Monitoring (C. Seatzu)	(to be decided)	Yes	9
C. Soft skill courses	/	/	/	0
D. Participation to seminars	/	/		0
E. Participation to international congresses or workshops	3 days conferences	(to be decided)		3
F. Presentation of research products at international congresses or workshops	1 presentation	(to be decided)		1
	TOTAL OF ECTS FOR TRAINING ACTIVITIES			17
G. Individual research activity	750 hours individual research activity	(to be decided)		30
H. Supervision of students	75 hours TA for Analysis and Control of Cyber-Physical Systems	(to be decided)		3
I. Integrative teaching activities	/	/		0
J. Preparation of manuscripts for conferences or journals	250 hours preparation of manuscripts for conferences or journals	(to be decided)		10
	TOTAL OF ECTS FOR RESEARCH ACTIVITIES			43
	TOTAL OF ECTS			60

Third academic year (planned)

	Description	Period	Final Exam	ECTS
A. Ph.D. courses	SIDRA PhD School	(to be decided)	Yes	4
B. Master's degree courses	(to be decided)	(to be decided)	(to be decided)	6
C. Soft skill courses	/	/	/	0
D. Participation to seminars	0	/		0
E. Participation to international congresses or workshops	3 days conferences	(to be decided)		3
F. Presentation of research products at international congresses or workshops	1 presentation	(to be decided)		1

	TOTAL OF ECTS FOR TRAINING ACTIVITIES			14
G. Individual research activity	775 hours individual research activity	(to be decided)		31
H. Supervision of students	75 hours TA for Analysis and Control of Cyber-Physical Systems	(to be decided)		3
I. Integrative teaching activities	/	/		0
J. Preparation of manuscripts for conferences or journals	300 hours preparation of manuscripts for conferences or journals	(to be decided)		12
	TOTAL OF ECTS FOR RESEARCH ACTIVITIES			46
	TOTAL OF ECTS			60

4. List of the publications written by the candidate in the triennium

International Journal Articles

International Conference Proceedings

Yike LI

Prof. Alessandro Giua